DEUTSCHE BUNDESBANK
EUROSYSTEM

Leitfaden für

TARGET2-Nutzer

Version 8.1

April 2015

Leitfaden

Inhalt

0 Vorwort 8

1 Einleitung 8

1.1 Benutzerhinweise für den TARGET2-Leitfaden 9

1.2 Weitere wichtige Dokumente 10

2 Allgemeines 13

2.1 Was ist TARGET2? 13

2.2 Was ist TARGET2-Securites? 13

2.2.1 Die Rolle der Zentralbanken im Kontext von TARGET2-Securities 17

2.2.2 Die Rollen der Banken im Rahmen von TARGET2-Securities 18

2.3 TARGET2-Struktur 18

2.3.1 Leitungsstruktur (Governance) 18

2.3.2 Technische Struktur 19

2.3.3 Organisationsstruktur auf der Ebene der Zentralbanken 21

2.4 Kommunikation mit den Nutzern 21

2.4.1 Kommunikationsmittel 22

2.5 Öffnungstage 24

2.6 Tagesablauf 26

2.7 Transaktionen über TARGET2 29

2.8 Liquiditätsströme zwischen PM-Konten und Geldkonten sowie zwischen Geldkonten 31

2.9 Nachrichtenfluss 38

2.10 Abwicklung von Nebensystemen 41

3 Teilnahme 44

3.1 Zugangskriterien 44

3.1.1 Direkte Teilnahme 44

3.1.2 Indirekte Teilnahme 46

3.1.3 Multi-Adressaten-Zugang 46

3.1.4 Erreichbare BIC-Inhaber 47

3.1.5 Kontengruppe 47

3.2 Internetbasierter Zugang 48

3.3 Anbindung und Registrierung 50

3.3.1 Anbindung an die Gemeinschaftsplattform 50

3.3.2 Anbindung an die T2S-Plattform 51

3.3.3 Erhebung von Stammdaten 51

3.3.3.1 Konfliktäre Registrierung von erreichbaren BIC-Inhabern und indirekten Teilnehmern 53

Inhalt

3.3.3.2 TARGET2-Directory ... 54
3.3.3.3 Auf der T2S-Plattform aufgeführte externe RTGS-Konten ... 56
3.3.3.4 Informationsfluss zwischen Zentralbanken, DCA-Inhabern und Zentralverwahrern ... 56
3.3.3.5 Verwaltung der Zugriffsrechte von direkt angeschlossenen DCA-Inhabern ... 57
3.4 Zertifizierungstests ... 59
3.5 Maßnahmen zur Gewährleistung der Sicherheit und operationellen Zuverlässigkeit von TARGET2-Nutzern ... 60
3.5.1 Aufgaben und Zuständigkeiten ... 60
3.5.2 Kritische und nichtkritische Teilnehmer ... 64
3.5.2.1 Kreditinstitute ... 65
3.5.2.2 Nebensysteme ... 66
3.5.2.3 „Servicebüro“ und „Mitglied/Konzentrator“ ... 68
3.5.3 Maßnahmen zur Gewährleistung der Sicherheit und operationellen Zuverlässigkeit von Nutzern ... 69
3.5.3.1 Für kritische und nichtkritische Teilnehmer anzuwendende Maßnahmen ... 69
3.5.3.2 Nur für kritische Teilnehmer anzuwendende Maßnahmen ... 71
3.5.4 Umsetzung ... 75
3.5.4.1 Rechtliche Durchsetzbarkeit ... 75
3.5.4.2 Übergangsphase ... 75
3.5.4.3 Konstruktiver Ansatz ... 76
3.5.5 Kommunikation und Koordinierung ... 76
3.5.6 Vertraulichkeit ... 76
3.5.7 Berichterstattung ... 77
3.5.8 Überprüfungsklausel ... 77
3.6 Beendigung oder Suspendierung der Teilnahme eines TARGET2-Teilnehmers ... 78
3.6.1 Auswirkungen der Suspendierung eines PM-Kontoinhabers ... 79
3.6.2 Auswirkungen der Suspendierung eines DCA-Inhabers ... 80
3.6.3 Auswirkungen der Suspendierung eines HAM-Teilnehmers ... 81
3.7 Vorläufiger oder endgültiger Ausschluss oder Beschränkung des Zugangs zu Innertageskrediten und/oder Selbstbesicherungsfazilitäten ... 81
3.8 Rechnungsstellung in TARGET2 ... 83
4. Der Geschäftstag im Normalbetrieb ... 84
4.1 Beginn des Geschäftstags ... 84
4.2 Liquiditätsbereitstellung ... 85
4.3 Nachtverarbeitung auf der Gemeinschaftsplattform ... 86
4.4 Geldrelevante Aspekte der T2S-Nachtverarbeitung ... 88

Inhalt

4.5 Betriebsfenster 90
4.6 SSP-Tagverarbeitung 90
4.7 Geldrelevante Aspekte der T2S-Nachtverarbeitung 92
4.8 Tagesendeverarbeitung 96
5. Grundsätzliche Aspekte der Verfahren für Ausnahmesituationen 97
5.1 Definition einer Störung 97
5.2 Verfahren zur Störungsbehebung 98
5.3 Kommunikation bei Störungen 98
6. Verfahren zur Handhabung von Störungen der Gemeinschaftsplattform 100
6.1 Verfahren bei Störungen zu Tagesbeginn (18.45 Uhr - 19.00 Uhr) 100
6.2 Verfahren bei Störungen der Nachtverarbeitung (19.00 Uhr – 22.00 Uhr und 1.00 Uhr – 7.00 Uhr) 100
6.3 Betriebsfenster (6.45 Uhr - 7.00 Uhr) 101
6.4 Verfahren bei Störungen der Tagverarbeitung (7.00 Uhr - 18.00 Uhr) 101
6.4.1 Fortsetzung des Geschäftsbetriebs (Business Continuity) 101
6.4.1.1 Intraregionale Ausfallsicherung 102
6.4.1.2 Interregionale Ausfallsicherung 102
6.4.2 Contingency-Abwicklung unter Einsatz des Contingency-Moduls 104
6.4.2.1 Aktivierungsverfahren für das Contingency-Modul 105
6.4.2.2 Zahlungsabwicklung im Contingency-Modul 106
6.4.2.3 Weitere Einzelheiten zur Nutzung des Contingency-Moduls 107
6.4.3 Verlängerung des Annahmeschlusses 110
6.4.3.1 Verschiebung des Annahmeschlusses aufgrund eines zuvor aufgetretenen SSP-Ausfalls 111
6.4.3.2 Verzögerter Annahmeschluss aufgrund einer anhaltenden SSP-Störung 111
6.5 Verfahren bei Störungen am Tagesende (18.00 Uhr - 18.45 Uhr) 114
7 Störungen auf der T2S-Ebene 116
7.1 Auswirkungen auf TARGET2 116
7.2 Situation einer T2S-Ausfallsicherung 117
8 Andere Ausfälle 119
8.1 Störungen auf der Zentralbankebene 119
8.1.1 Ausfall einer Zentralbank 119
8.1.2 Ausfall eines proprietären Heimatkontos (PHA) 120
8.2 Betriebs- oder technische Störungen auf Teilnehmerebene 122
8.3 Ausfall eines Nebensystems 125

Inhalt

8.3.1 Nebensysteme, die die Nebensystem-Schnittstelle nutzen ... 126
8.3 2 Nebensysteme, die die Zahlungsschnittstelle nutzen ... 128
8.4 Technische Suspendierung ... 128
8.5 Ausfall von SWIFT ... 129
8.5.1 Verarbeitung von Zahlungen ... 130
8.5.2 Verarbeitung von Dateien aus Nebensystemen ... 131
9. Test der Contingency- und Business-Continuity-Maßnahmen ... 132
9.1 Geltungsbereich ... 132
9.2 Ziel der Tests ... 132
9.3 Funktionen und Zuständigkeiten ... 132
9.4 Testumgebung ... 133
9.5 Häufigkeit und Planung ... 133
9.6 Testergebnisse und -berichte ... 133
9.7 Test der Contingency-Maßnahmen ... 134
9.7.1 Kritische Teilnehmer ... 134
9.7.2 Gemeinschaftsplattform (Testen der Contingency-Module) ... 135
9.8 Test der Business-Continuity-Maßnahmen ... 136
9.8.1 Kritische Teilnehmer ... 136
9.8.2 SSP 137
10. Change- und Release-Management-Verfahren ... 138
10.1 Jährliches Release ... 138
10.1.1 Wichtige Termine ... 138
10.1.2 Einbindung der Nutzer ... 139
10.1.3 Priorisierung und Entscheidungsfindung ... 140
10.2 Notfalländerungen und Hot Fixes ... 140
10.2.1 Notfalländerungen ... 141
10.2.2 Hot Fixes ... 141
11. TARGET2-Ausgleichsregelung ... 142
11.1 Allgemeines ... 142
11.2 Verfahrensregeln ... 142
Anhang I SSP Interregionale Ausfallsicherung mit Datenverlust ... 144
Anhang II Störungsbericht für TARGET2-Nutzer ... 148
Anhang III Selbstzertifizierungserklärung ... 150
Anhang IV Formular für Änderungsvorschläge ... 163
Anhang V Glossar und Abkürzungsverzeichnis ... 165

Verzeichnis der Abbildungen, Tabellen und Kästen

Abbildungen

Abbildung 1: Die vier Rollen der Zentralbanken im Rahmen von T2S 18
Abbildung 2: TARGET2-Struktur 20
Abbildung 3: Überblick über die TARGET2-Beteiligten 21
Abbildung 4: Informationsfluss 24
Abbildung 5: TARGET2 und T2S-Feiertage 25
Abbildung 6: Bewegungen auf Geldkonten 31
Abbildung 7: Liquiditätsströme zwischen PM-Konten und Geldkonten 32
Abbildung 8 Euro-Zwischenkonten 35
Abbildung 9: Transaktionsfluss in Y-Copy 39
Abbildung 10: Liquiditätsübertragung von T2S auf TARGET2 (ISO 20022 Nachrichtenströme) 41
Abbildung 11: Hierarchie-Modell der T2S-Parties 58
Abbildung 12: Abwicklungsverfahren 6 87
Abbildung 13: T2S-Nachtverarbeitungssequenzen 89
Abbildung 14: Automatische Rückführung der Zentralbank-Selbstbesicherung 95
Abbildung 15: Als mögliche Störquellen ermittelte Beteiligte 97
Abbildung 16: Zwei Regionen, vier Standorte 101
Abbildung 17: Abläufe am Tag der Störung 112
Abbildung 18: Ablauf am Tag nach der Störung 113
Abbildung 19: Überblick über die Abläufe im Fall einer Störung 114
Abbildung 20: Abläufe nach einer interregionalen Ausfallsicherung mit Datenverlust 147

Tabellen

Tabelle 1: TARGET2-Leitungsstruktur 19
Tabelle 2: Zeitplan an einem Geschäftstag 27
Tabelle 3: Liquiditätsüberträge - Überblick 34
Tabelle 4: Liquiditätsübertragung zwischen Geldkonten und PM-Konten 37
Tabelle 5: Abwicklungsverfahren 42
Tabelle 6: TARGET2-Teilnahmestruktur 47
Tabelle 7: TARGET2-Directory 55
Tabelle 8: Zuständigkeit der Zentralbank für direkte Teilnehmer 63
Tabelle 9: Abschluss der T2S-Echtzeitabwicklung 93
Tabelle 10: Behandlung von Nebensystem-Transaktionen 104

Verzeichnis der Abbildungen, Tabellen und Kästen

Tabelle 11: Auswirkungen einer T2S-Störung auf TARGET2 116
Tabelle 12: Auswirkungen eines Zentralbankausfalls 120
Tabelle 13: Auswirkungen eines PHA-Ausfalls 122
Tabelle 14: Zeitplan für das jährliche Release 139

Kästen

Kasten 1: Euro-Zwischenkonten 35
Kasten 2: Datenfeeds für die Client Auto-Collateralisation 85
Kasten 3: Automatisierte Rückführung der Zentralbank-Selbstbesicherung 94
Kasten 4: Das Konzept (sehr) kritischer TARGET2-Zahlungen 108
Kasten 5: Aspekte, die bei der Entscheidung über kritische Zahlungen zu berücksichtigen sind 109
Kasten 6: Contingency-Zahlungen 124

0 Vorwort

Das vorliegende Dokument ist eine Übersetzung des englischen Originaltextes durch die Deutsche Bundesbank.

Der englische und rechtlich verbindliche Originaltext ist auf der Homepage der Deutschen Bundesbank als pdf-Download verfügbar. Dort ist ebenfalls diese Übersetzung als pdf-Datei abrufbar.

1 Einleitung

Der vorliegende „Leitfaden für TARGET2-Nutzer" (nachfolgend „TARGET2-Leitfaden") versteht sich als Standardwerk für TARGET2-Nutzer (Kreditinstitute, Nebensysteme und sonstige Einrichtungen, die Zahlungen in TARGET2 abwickeln[1]), das ihnen ein besseres Verständnis der allgemeinen Funktionsweise des TARGET2-Systems und eine möglichst effiziente Nutzung ermöglichen soll. In dem Leitfaden sollen sämtliche operativen Aspekte im Zusammenhang mit der alltäglichen TARGET2-Nutzung einschließlich der Geldverrechnung über TARGET2-Securities (T2S) in Euro behandelt werden, um einen reibungslosen Betrieb zu gewährleisten.

Außerdem stellt der TARGET2-Leitfaden die Funktionalität des Gesamtsystems sowie die Besonderheiten im Hinblick auf die einzelnen Zentralbanken dar, d. h. die nationalen Zentralbanken im Euroraum (NZBen), die Europäische Zentralbank (EZB) und sonstige nationale Zentralbanken, die an TARGET2 angeschlossen sind. Dokumentiert sind die zentralbankspezifischen Besonderheiten auf der Website der jeweiligen nationalen Notenbank.

Der TARGET2-Leitfaden wurde so konzipiert, dass er wann immer erforderlich aktualisierbar ist und sowohl die Zentralbanken einschließlich der drei bzw. vier Anbieter-Zentralbanken (3ZB/4ZB)[2] wie auch die TARGET2-Nutzer an seiner Ausgestaltung mitwirken können. Er ist als ein dynamisches Dokument gedacht, in dem Aktualisierungen aufgegriffen werden, die entweder von nationalen TARGET2-Nutzergruppen ausgehen, aus vom Europäischen System der Zentralbanken (ESZB) für TARGET2-Nutzer auf Euroraumebene organisierten Veranstaltungen resultieren oder aus operativen Erfahrungen und neuen Systemversionen rühren.

1 Nähere Informationen finden sich in Kapitel 3 („Teilnahme").

2 Die 3ZB sind die technischen Anbieter der Gemeinschaftsplattform: Banca d'Italia, Banque de France und Deutsche Bundesbank. Bei den 4ZB handelt es sich um die technischen Anbieter der T2S-Plattform: Banca d'Italia, Banque de France, Deutsche Bundesbank und Banco de España

Es ist durchaus denkbar, dass der Leitfaden auch für andere mit TARGET2 befasste Gruppen oder für die Öffentlichkeit von Interesse ist, weshalb er auf der TARGET2-Website (www.target2.eu) zur Verfügung steht.

Aus dem Inhalt des Leitfadens leiten sich keinerlei Rechte für TARGET2-Nutzer und sonstige natürliche oder juristische Personen bzw. Rechte hinsichtlich der Abwicklung der Geschäfte ab. Die Zeitangaben im Dokument beziehen sich auf die Ortszeit am Sitz der Europäischen Zentralbank.

1.1 Benutzerhinweise für den TARGET2-Leitfaden

Der Leitfaden soll TARGET2-Nutzern bei den täglichen Betriebsabläufen als Referenz dienen und liefert darüber hinaus Hinweise, welche weiteren Dokumente für die Nutzer von wichtigem Interesse sein könnten und wo diese zu finden sind.

Kapitel 2 („Allgemeines") bietet eine Darstellung von TARGET2 und TARGET2-Securities, der Leitungs- und technischen Struktur von TARGET2, der Organisationsstruktur auf Zentralbankebene, der Kommunikation mit den Nutzern, der Öffnungstage und des Zeitplans an einem Geschäftstag, der über TARGET2durchgeführten Transaktionen sowie der Abwicklung von Nebensystemen.

Kapitel 3 („Teilnahme") erläutert die Teilnahmevoraussetzungen, das Vorgehen zur Beantragung und zur Registrierung (vor allem im Hinblick auf die Stammdatenerhebung), die Zertifizierungstests, die Maßnahmen zur Gewährleistung von Sicherheit und operationeller Zuverlässigkeit, die Kündigung oder Suspendierung von TARGET2-Nutzern sowie die Rechnungsstellung in TARGET2.

In Kapitel 4 werden die Abläufe der unterschiedlichen Phasen eines normalen Geschäftstages dargelegt. Kapitel 5, Kapitel 6, Kapitel 7 und Kapitel 8 beschäftigen sich mit den Verfahren, die bei außergewöhnlichen Ereignissen anzuwenden sind. Dabei wählen Kapitel 4 bis 8 eine chronologische Darstellung der Abläufe während eines Geschäftstags, d. h., zunächst werden die Verfahren zu Beginn des Betriebstags (am Abend des vorherigen Werktags), gefolgt von der Nachtverarbeitung, der Tagesverarbeitung und schließlich der Tagesendeverarbeitung, erläutert.

Kapitel 9 beschreibt die Testanforderungen, die für die Notfallmaßnahmen (Contingency) und für die Vorkehrungen zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity) gelten. Kapitel 10 erläutert das Change Management mit Blick auf die jährlichen TARGET2-Releases sowie die Notfalländerungen und sogenannten Hot Fixes. Eine Beschreibung der Verfahren zur TARGET2-Ausgleichsregelung findet sich in Kapitel 11.

Die Anhänge des Leitfadens enthalten eingehende Informationen zum Wiederherstellungsprozess bei einer interregionalen Ausfallsicherung mit Datenverlust in TARGET2 (Anhang I), einen

Störungsbericht (Anhang II), die Selbstzertifizierungserklärung für kritische Teilnehmer (Anhang III) und ein Formular für Änderungsvorschläge (Anhang IV) sowie ein Glossar einschließlich Abkürzungsverzeichnis (Anhang V).

Zeitangaben in diesem Dokument beziehen sich auf die Ortszeit am Sitz der Europäischen Zentralbank, also Mitteleuropäische Zeit (MEZ).

1.2 Weitere wichtige Dokumente

Rechtliche Dokumentation (abrufbar auf der EZB-Website)

- TARGET2-Leitlinie (einschließlich nachfolgender Änderungsleitlinien)

Die TARGET2-Leitlinie (EZB/2012/27) stellt das rechtliche Rahmenwerk für TARGET2 dar, mit dem der TARGET2-Leitfaden in vollem Einklang stehen muss. Sie umfasst in ihrem Geltungsbereich unter anderem die auf Euro lautenden T2S-Geldkonten, während sonstige T2S-Aspekte in der T2S-Leitlinie (ECB/2012/13) abgedeckt werden.

Die TARGET2-Leitlinie richtet sich an Zentralbanken und basiert, obgleich er dezentral von jeder Notenbank selbst umzusetzen ist, auf dem Prinzip höchstmöglicher Harmonisierung. In den Anhängen werden die Governance, die harmonisierten Bedingungen für TARGET2-Teilnehmer und die Innertageskredit-/Selbstbesicherungsfazilitäten abgehandelt.

- Harmonisierte Bedingungen

Jede teilnehmende Zentralbank erlässt Regelungen zur Umsetzung der harmonisierten Bedingungen für die Teilnahme an TARGET2,[3] die in der TARGET2-Leitlinie niedergelegt sind und ausschließlich das Verhältnis zwischen der betreffenden nationalen Zentralbank und ihren TARGET2-Nutzern regeln.

Die harmonisierten Bedingungen, die für die TARGET2-Nutzer gelten, enthalten eine Darstellung von TARGET2 und erläutern unter anderem Zugangsvoraussetzungen, Kontenverwaltung, Abwicklung von Zahlungsaufträgen, Rechte und Pflichten der Parteien sowie Finalität und Haftung. In ihren Anhängen bieten sie ferner technische Spezifikationen zur Verarbeitung von Zahlungsaufträgen, Muster für Rechtsfähigkeits- bzw. Ländergutachten sowie das Gebührenverzeichnis und erläutern

[3] Harmonisierte Bedingungen für die Eröffnung und Führung eines PM-Kontos in TARGET2 (vgl. Anhang II), Ergänzende und geänderte harmonisierte Bedingungen für die Eröffnung und Führung eines PM-Kontos in TARGET2 im Rahmen des internet-basierten Zugangs(vgl. Anhang V), und die harmonisierten Bedingungen für die Eröffnung und Führung eines Geldkontos in TARGET2 (siehe Anhang IIa).

unter anderem Betriebszeiten, Notfallverfahren, die Modalitäten des Liquiditätspooling und die Ausgleichsregelung.

Betriebsdokumentation (abrufbar auf der TARGET2-Website)

- User guide for collection of static data and Registration Guide for DCA holders

Hier finden potenzielle TARGET2-Nutzer alle zum Ausfüllen der Registrierungsformulare erforderliche Informationen.

- User information guide to the TARGET2 pricing

Dieses Dokument enthält detaillierte Angaben zur Preisgestaltung und Rechnungsstellung in TARGET2.

- Settlement times of ancillary systems

Dieses Dokument enthält vor allem Erläuterungen zu den Verarbeitungszeiten der Nebensysteme.

Spezifikationen (abrufbar auf der TARGET2-Website)

- TARGET2 General Functional Specifications (GFS) and TARGET2 User Detailed Functional Specifications (UDFS).

Diese Dokumente enthalten technische Einzelheiten zur Funktionsweise der Gemeinschaftsplattform (Single Shared Platform – SSP).

- ICM User Handbook

Dieses Handbuch liefert detaillierte Angaben zur Funktionsweise des Informations- und Steuerungsmoduls (Information and Control Module - ICM).

- Benutzerhandbuch zur Public-Key-Zertifizierung für den Internetzugang (User manual internet access for the public key certification service)

In diesem Handbuch werden die Verfahren beschrieben, welche die Banca d'Italia als akkreditierte Zertifizierungsstelle für die Ausstellung und Verwendung elektronischer Zertifikate im Rahmen des internetbasierten Zugangs zu TARGET2 einsetzt. Die Dienstleistung wird im Auftrag des Eurosystems von der Banca d'Italia erbracht.

- SWIFT-Dokumentation

Die SWIFT-Dokumentation liefert Einzelheiten zu den unterschiedlichen SWIFT-Standards, abrufbar auf der SWIFT-Website

- Dokumente zu TARGET2-Securities

Von besonderer Bedeutung sind die T2S-Nutzerfeinspezifikationen (User Detailed Functional Specifications – UDFS), das Handbuch für T2S-Nutzer (T2S User Handbook – UHB) und die Definitionen zur Nutzeranforderung (User Requirement Definitions – URD), die auf der T2S-Website veröffentlicht sind.

Die oben genannten Dokumente stehen auf der TARGET2-Website der Deutschen Bundesbank (http://www.bundesbank.de) zur Verfügung. Außerdem sind dort weitere Informationen zu bestimmten nationalen Besonderheiten und Verfahren veröffentlicht.

2 Allgemeines

2.1 Was ist TARGET2?

TARGET2 (Trans-European Automated Real-time Gross settlement Express Transfer, zweite Systemgeneration) bezeichnet das Individualzahlungssystem des Eurosystems. Es wurde entwickelt, um die Festlegung und Durchführung der Geldpolitik im Euroraum und die Förderung einer reibungslosen Funktionsweise der Zahlungssysteme im Rahmen der Zielsetzung des Eurosystems zu unterstützen und damit zur Integration und Stabilität des Euro-Geldmarkts beizutragen.

Technisch wird TARGET2 auf einer einzigen Gemeinschaftsplattform (SSP)[4] betrieben, über die allen Nutzern dasselbe Leistungsspektrum zur Verfügung steht. TARGET2 ist so ausgelegt und konstruiert, dass es höchste Ansprüche an die Systemstabilität und -zuverlässigkeit erfüllt und grenzüberschreitende Euro-Zahlungen ebenso reibungslos wie inländische Zahlungen verarbeitet. TARGET2 wickelt ausschließlich auf Euro lautende Zahlungsaufträge – vor allem Großzahlungen wie z. B. Zahlungen im Zusammenhang mit Devisen-, Wertpapier- und Geldmarktgeschäften – ab, die kostengünstig, äußerst sicher und in sehr kurzer Verarbeitungszeit ausgeführt werden.

Es handelt sich um ein Echtzeit-Bruttosystem (Real-Time Gross Settlement System – RTGS), bei dem Zahlungen individuell abwickelt werden: Zahlungsaufträge werden in einem kontinuierlichen automatisierten Verfahren einzelnd verarbeitet. Damit gewährleistet TARGET2 eine umgehende Abwicklung mit sofortiger Finalität aller Zahlungen, vorausgesetzt der Zahlungspflichtige verfügt auf seinem Konto bei der Zentralbank über ausreichendes Guthaben bzw. hinreichende Überziehungsfazilitäten,[5] wobei für TARGET2-Zahlungen keine Mindestbeträge vorgeschrieben sind.

Zudem beinhaltet TARGET2 **auf Euro lautende Geldkonten (Dedicated Cash Accounts – DCAs)**, die technisch auf der T2S-Plattform angesiedelt sind (siehe Zusatzinformationen unten).

2.2 Was ist TARGET2-Securites?

Eine weitere wichtige Infrastruktur, die Abhängigkeiten mit TARGET2 hat, ist TARGET2-Securities (T2S). Das Eurosystem stellt T2S-Dienstleistungen über die von den 4ZB – der Deutschen

[4] SSP (Single Shared Platform) bezeichnet die technische Plattform, auf der die TARGET2-bezogenen Dienstleistungen bereitgestellt werden. Dienste in Zusammenhang mit TARGET2-Securities werden über die T2S-Plattform erbracht.

[5] Mit einigen Ausnahmen wie z. B. gespeicherten Zahlungsaufträgen (warehoused payments) oder Zahlungen an einen suspendierten Teilnehmer.

Bundesbank, der Banque de France, der Banca d'Italia und der Banco de España – errichteten und betriebenen T2S-Plattform bereit.

T2S ermöglicht Zentralverwahrern (Central Securities Depositories - CSDs) national wie auch grenzüberschreitend eine harmonisierte und standardisierte Abwicklung von Wertpapiertransaktionen. Mit T2S gilt ein einheitlicher Regel-, Normen- und Gebührenkatalog für alle Zentralverwahrer, die zur Abwicklung ihrer Wertpapiertransaktionen die T2S-Plattform nutzen. Auch die geldliche Verrechnung erfolgt in Zentralbankgeld und unterliegt einheitlichen Regeln und Standards.

T2S integriert die von den Marktteilnehmern bei einem bzw. mehreren Zentralverwahrern unterhaltenen Wertpapierkonten und die bei den jeweiligen Zentralbanken unterhaltenen Geldkonten (DCAs) auf einer gemeinsamen technischen Plattform.

Konzipiert ist T2S als ein Multiwährungssystem. Dabei ist der Euro die erste Währung, in der Wertpapiertransaktionen auf der T2S-Plattform abgewickelt werden. Somit sind T2S und TARGET2 im Hinblick auf die Euro-Liquiditätssteuerung eng miteinander verzahnt. Die Verbindung von TARGET2 und T2S basiert auf einem „Application-to-Application-Ansatz", der durch die T2S-Schnittstelle (T2S Interface – T2SI) gewährleistet wird.

Anzumerken ist, dass sich der vorliegende Leitfaden nur mit auf Euro lautenden Transaktionen und Konten befasst.

Wichtige Aspekte im Zusammenhang mit T2S:

- Die in Euro denominierten Geldkonten (DCAs) fallen, obgleich sie technisch auf der T2S-Plattform angesiedelt sind, unter das rechtliche Rahmenwerk von TARGET2. Somit werden rechtliche Fragen in Zusammenhang mit den Geldkonten in der TARGET2-Leitlinie behandelt und die operativen Verfahren in Bezug auf die Geldkonten vom Leitfaden abgedeckt.
- Im Hinblick auf die Liquidität sind TARGET2 und T2S über sogenannte Zwischenkonten miteinander verknüpft, die den Liquiditätsaustausch zwischen Konten im Zahlungsverkehrsmodul (PM-Konten – Payments Module Accounts) und Geldkonten ermöglichen.
- Jede Einrichtung, die mindestens ein PM-Konto und/oder ein Geldkonto bei einer Zentralbank unterhält, ist ein TARGET2-Teilnehmer.
- Der Zugriff des Geldkontoinhabers oder des in dessen Namen handelnden Inhabers des PM-Hauptkontos (Main PM Account) auf das Geldkonto erfolgt *a)* über eine direkte Verbindung zur T2S-Plattform durch einen zugelassenen Mehrwertnetzwerkdienstleister (value-added network

service provider – VA-NSP) für T2S (direkt angeschlossene Geldkontoinhaber) und/oder *b)* über einen indirekten Anschluss durch die TARGET2-Zusatzleistungen (VAS) für T2S (indirekt angeschlossene Geldkontoinhaber).

- Vorbehaltlich der Erfüllung der einschlägigen Zulassungsvoraussetzungen kann eine Einrichtung ab der ersten T2S-Migrationswelle bei jeder Zentralbank ein Geldkonto in Euro eröffnen. Diese Regel gilt unabhängig davon, in welcher Migrationswelle der nationale Zentralverwahrer zu T2S überwechselt. Die Zulassungskriterien für die Eröffnung eines Geldkontos entsprechen – gemäß der TARGET2-Leitlinie – jenen für die Eröffnung eines PM-Kontos.
- Jedes Geldkonto muss mit einem einzigen PM-Konto, dem sog. PM-Hauptkonto verlinkt sein[6]. Allerdings ist es zulässig, dass mehrere Geldkonten mit ein- und demselben PM-(Haupt)konto verknüpft sind. Das PM-Hauptkonto kann in den Büchern derselben Zentralbank wie das Geldkonto eröffnet werden, was allerdings nicht zwingend ist.
- Der Geldkontoinhaber und der PM-Hauptkontoinhaber können unterschiedliche Einrichtungen sein (d. h., der Geldkontoinhaber braucht kein PM-Konto zu unterhalten, selbst wenn das Geldkonto mit einem PM-Konto verknüpft sein muss). Die vertragliche Vereinbarung zwischen dem Geldkontoinhaber und dem PM-Kontoinhaber liegt in deren eigener Verantwortung.
- Der Inhaber des PM-Hauptontos ist für die Zahlung der Gebühren der im Zusammenhang mit dem angeschlossenen Geldkonto erbrachten T2S-Dienstleistungen sowie für etwaige Strafentgelte im Falle einer Umbuchung von Sicherheiten (relocation of collateral) verantwortlich.
- Die Geldkonten (außer den von einer Zentralbank selbst unterhaltenen Geldkonten) können zu keinem Zeitpunkt einen Negativsaldo aufweisen. Außerdem muss der Saldo des Geldkontos am Tagesende auf null stehen. Realisiert wird dies durch den automatisierten Liquiditätstransfer („automated Cash-Sweep") der nach Annahmeschluss für eingehende Liquiditätsüberträge (um 17.45 Uhr) auf dem Geldkonto verbleibende Liquidität auf das PM-Hauptkonto transferiert. Dennoch wird DCA-Inhabern empfohlen, zur Wertpapierabwicklung nicht mehr benötigte Liquidität zu einem früheren Zeitpunkt von den Geldkonten auf die PM-Konten zu transferieren.
- Geldkontoinhaber können sich im Wege der Selbstbesicherung (Auto-Collateralisation) refinanzieren, d. h. durch einen von der Zentralbank gewährten Innertageskredit, der in Anspruch genommen wird, wenn die Liquidität auf den Geldkonten zur Abwicklung von Wertpapiertransaktionen nicht ausreicht. Dabei wird der Innertageskredit entweder mit

[6] Externes RTGS-Konto, das mit dem Geldkonto unter der GUI-Bildschirmanzeige „Static Data > Dedicated Cash Account" verlinkt ist.

Sicherheiten unterlegt, die vom Geldkontoinhaber gekauft werden („Collateral on flow"), oder mit Sicherheiten, die vom Geldkontoinhaber bereits gehalten werden und für die Auto-Collateralisation bestimmt und entsprechend gekennzeichnet sind („Collateral on stock").

- Um die Möglichkeit der Zentralbank-Selbstbesicherung zu nutzen, muss der Geldkontoinhaber ein PM-Konto mit Zugang zu Innertageskredit bei derselben Zentralbank unterhalten, bei der auch das DCA geführt wird.
- Inhaber von Geldkonten können ihren Kunden (z. B. Wertpapierkontoinhabern) Kredite einräumen, die automatisch durch die Funktion „Client Auto-Collateralisation" in T2S besichert werden. Die Client Auto-Collateralisation (Bereitstellung von Liquidität für Kunden) wird in Anspruch genommen, wenn das External Guarantee Limit des Kunden ausgeschöpft ist und Wertpapiertransaktionen nicht mehr abgewickelt werden können; dabei könnten entweder die Sicherheiten verwendet werden, die vom Kunden erworben werden („collateral on flow"), oder vom Kunden bereits gehaltene Wertpapiere, die für die Selbstbesicherung bestimmt und als solche gekennzeichnet sind („collateral on stock"). Falls ein Geldkontoinhaber Client-Auto-Collateralisation anbietet, muss er eine Liste mit Wertpapieren aufstellen, die als Sicherheiten akzeptiert werden („List of eligible securites" – Liste besicherungsfähiger Wertpapiere), sowie die entsprechenden Bewertungen (d. h., jene Preise, die T2S zur Bewertung der Sicherheitenpositionen verwenden kann). Nähere Informationen dazu finden sich in Kasten 2 im Abschnitt 4.1.
- Zentralbanken sind alleinverantwortlich für die Geschäftsbeziehung mit ihren Nutzern und sollten sich um alle Vorfälle, Fragen oder Probleme, die von diesen aufgeworfen werden, kümmern. Bei Konnektivitätsproblemen kann ein Geldkontoinhaber mit direkter T2S-Anbindung den T2S Service Desk allerdings direkt kontaktieren; dies ist auch umgekehrt der Fall (siehe Abschnitt 2.4).
- T2S ist kein Nebensystem und besitzt keinen Systemstatus (da T2S unter die rechtliche Abgrenzung von TARGET2 fällt, wird die Finalität im TARGET2-Leitfaden behandelt). Aus diesem Grund, aber auch wegen der engen Verknüpfung mit TARGET2, unterscheidet der Leitfaden zwischen den T2S-relevanten Bestimmungen und den Bestimmungen, die für das Nebensystem relevant sind.

2.2.1 Die Rolle der Zentralbanken im Kontext von TARGET2-Securities

Im Eurosystem lassen sich vier Rollen[7] unterscheiden, die die Zentralbanken im Rahmen von TARGET2-Securities ausfüllen:

- Rolle 1: **System-Entity** oder **Bank der Banken** – insbesondere bei der Geschäftsbeziehung mit den Banken im geldbezogenen Kontext und was die Eröffnung von Geldkonten betrifft.
- Rolle 2: **TARGET2-Systemeigner**, Status des Ausschusses für Zahlungs- und Verrechnungssysteme (Payment and Settlement Systems Committee – PSSC) in Verbindung mit der Zentralbankrolle als an TARGET2 teilnehmende Zentralbank. Was die Leitung bzw. Governance betrifft, so verfügt der EZB-Rat (sog. Ebene 1 oder E1) über die oberste Zuständigkeit für TARGET2, während die Zentralbanken des Eurosystems (Ebene 2 oder E2) als Kollektiv eine subsidiäre Kompetenz in von der Ebene 1 delegierten Fragen besitzen. Repräsentanten der Ebene 2 sind Mitglieder des PSSC.
- Rolle 3: Als **Sicherheitenverwalter** haben die Zentralbanken die Zuständigkeit dafür, wie im Eurosystem mit der Besicherung der geldpolitischen Geschäfte, der Innertageskredite und mit den Selbstbesicherungsfazilitäten (Auto-Collateralisation) zu verfahren ist.
- Rolle 4: **Settlement Agent** – betrifft insbesondere die Abwicklung der eigenen Geschäfte in der Funktion als Kunde eines Zentralverwahrers (CSD-Teilnehmer).

In diesem Dokument werden die Rollen eins und zwei behandelt, die für den Leitfaden von besonderer Bedeutung sind (in Abbildung 1 rot umrahmt). Auf Rolle 3 und Rolle 4 wird hier nicht näher eingegangen.

[7] Partielle Überlappungen der unterschiedlichen Rollen sind möglich. Die Rolle der Zentralbanken als Betreiber von Wertpapierabwicklungssystemen/Zentralverwahrer (z. B. in Belgien und Griechenland) bleibt unberücksichtigt.

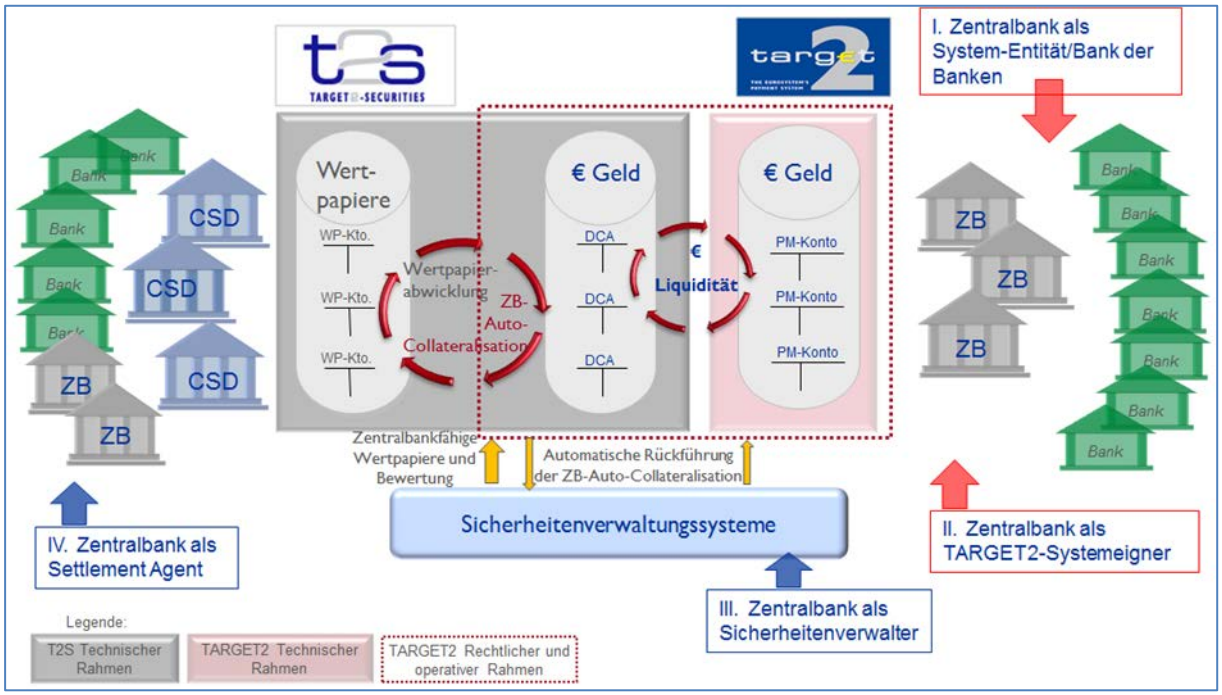


Abbildung 1: Die vier Rollen der Zentralbanken im Rahmen von T2S

2.2.2 Die Rollen der Banken im Rahmen von TARGET2-Securities

Eine Bank kann im Kontext von T2S die folgenden Rollen einnehmen:

- Geldkontoinhaber, d. h. Inhaber eines oder mehrerer DCAs
- CSD-Teilnehmer, d. h., Inhaber von Wertpapierkonten bei einem oder mehreren Zentralverwahrern;
- Liquiditätsbereitsteller, d. h., als Institut, das die Abwicklung von Wertpapiertransaktionen seiner Kunden (CSD-Teilnehmer) auf seinem Geldkonto ermöglicht oder als Institut, das über sein PM-Konto Liquidität für ein Geldkonto eines anderen Instituts bereitstellt;
- als Kreditgeber, d. h. als Institut, das Innertageskredite über die Client Auto-Collateralisation an seine Kunden (CSD-Teilnehmer) ausreicht.

2.3 TARGET2-Struktur

2.3.1 Leitungsstruktur (Governance)

Das TARGET2-Management beruht auf einer dreistufigen Leitungsstruktur. Die Aufgaben dabei vom EZB-Rat (Ebene 1), den Zentralbanken des Eurosystems (Ebene 2) und den Anbieter-Zentralbanken

(Ebene 3) wahrgenommen. Der **EZB-Rat** ist für die allgemeine Leitung von TARGET2 zuständig. Die Aufgaben der Ebene 1 fallen in die ausschließliche Zuständigkeit des EZB-Rates. Der Ausschuss für Zahlungs- und Verrechnungssysteme des ESZB (PSSC) unterstützt den EZB-Rat als beratendes Gremium in allen Angelegenheiten, die Bezug zu TARGET2 haben. Die Zentralbanken des Eurosystems sind innerhalb des vom EZB-Rat festgelegten allgemeinen Rahmens für die Aufgaben der Ebene 2 zuständig. Neben seiner beratenden Funktion nimmt der Ausschuss für Zahlungs- und Verrechnungssysteme die Aufgaben der Ebene 2 wahr. Die Anbieter-Zentralbanken (Ebene 3) treffen Entscheidungen zum täglichen Betrieb der Gemeinschaftsplattform (SSP) auf der Grundlage eines vorab definierten Service Level Agreements.

Ebene 1 **EZB-Rat**	**Ebene 2** **Zentralbanken des Eurosystems**	**Ebene 3** **Anbieter-Zentralbanken**
- Steuerung im Fall ernster Krisensituationen - Genehmigung der Einrichtung und des Betriebs des TARGET2-Simulators - Benennung der Zertifizierungsstellen für den internetbasierten Zugang - Festlegung der Sicherheitspolitik, -anforderungen und -kontrollen für die SSP - Festlegung der Grundsätze für die Sicherheit der Zertifikate für den internetbasierten Zugang	- Management im Hinblick auf die Zuständigkeiten des Systemeigners (auch in Krisensituationen) - Kontakt mit Nutzern auf europäischer Ebene (unter Beachtung der ausschließlichen Verantwortung der Zentralbanken für die Geschäftsbeziehung zu ihren TARGET2-Nutzern) und Überwachung der täglichen Nutzeraktivitäten aus geschäftspolitischer Sicht (Aufgabe der Zentralbanken) - Überwachung der Geschäftsentwicklungen - Budgetierung, Finanzierung, Rechnungsstellung (Aufgabe der Zentralbanken) und sonstige administrativen Aufgaben	- Betrieb der SSP auf der Grundlage der in der TARGET2-Leitlinie genannten Vereinbarung

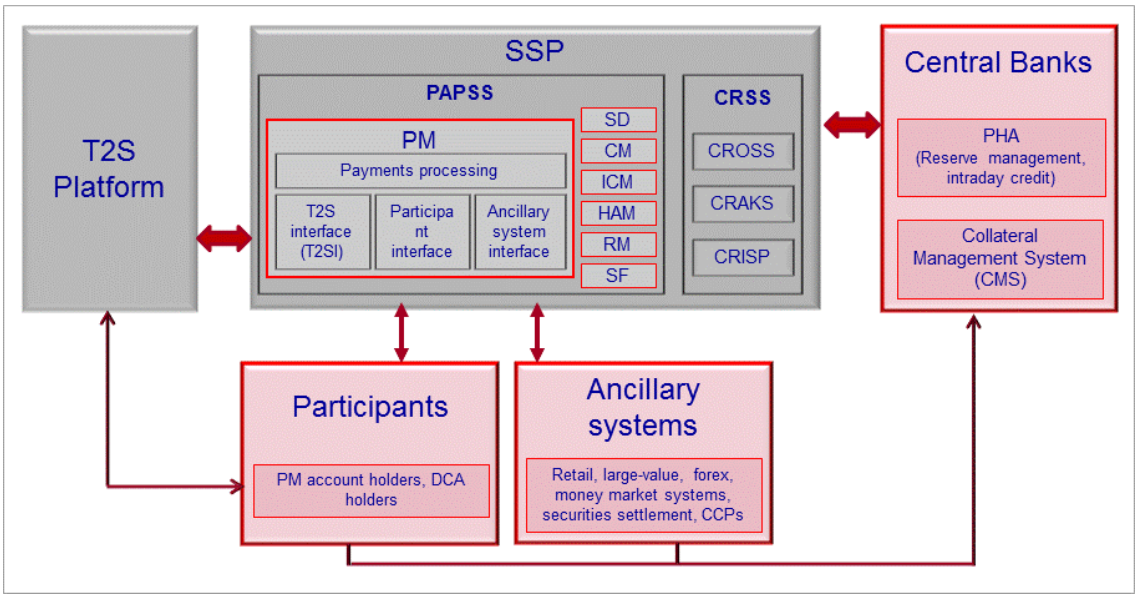
Tabelle 1: TARGET2-Leitungsstruktur

2.3.2 Technische Struktur

Was die technische Struktur betrifft, so weist TARGET2 folgende Merkmale auf:

- die Gemeinschaftsplattform (Single Shared Platform – SSP) mit dem Zahlungsabwicklungs- und Kontoführungssystem (Payment and Accounting Processing Services Systems – PAPSS) und dem Kundenbetreuungssystem (Customer Related Services System – CRSS)

- das PAPSS mit dem Zahlungsmodul (Payments Module – PM), das Modul für die ständigen Fazilitäten (Standing Facilities Module – SF), das Modul für die Mindestreserveverwaltung (Reserve Management Module – RM), das Heimatkontomodul (Home Accounting Module – HAM), das Stammdatenmodul (Static Data Module – SD), das Contingency-Modul (CM) und dem Informations- und Steuerungsmodul (Information and Control Module – ICM)
- die ausschließlich für die Zentralbanken bestimmten Kundenbetreuungssysteme (CRSS-Hauptmeldefunktionen und CRISP – Consumption Report and Invoicing Support Process)
- die T2S-Schnittstelle (T2SI), die TARGET2 mit T2S verbindet. Die gemeinsame Systemschnittstelle basiert auf dem internen 4ZB-Netzwerk und nutzt den, in den T2S-Anforderungen festgelegten, XML-Nachrichtenstandard
- die Zentralbanken mit einer proprietären Anwendung für die Heimatkonten (Proprietary Home Account Application – PHA), Mindestreserveverwaltung und Innertageskredit
- die Kreditinstitute und sonstigen in TARGET2 abwickelnden Einrichtungen (außer Nebensysteme), die über SWIFT oder Internet an die Gemeinschaftsplattform und/oder an die T2S-Plattform über die lizensierten Mehrwertnetzwerkdienstleister (Value-Added Network Service Providers – VA-NSP) angeschlossen sind



- die Nebensysteme, die über SWIFT an die SSP angebunden sind.

Abbildung 2: TARGET2-Struktur

2.3.3 Organisationsstruktur auf der Ebene der Zentralbanken

Jede Zentralbank verfügt über einen **National Service Desk**, der als Ansprechpartner für die jeweiligen TARGET2-Nutzer fungiert. Im TARGET-2 Rahmenwerk wird der National Service Desk durch die **Settlement-Manager** vertreten, die für die Verwaltung des täglichen Geschäftsbetriebs verantwortlich sind. Alle Settlement-Manager sind durch ein voreingestelltes Telekonferenzsystem („TARGET2 Settlement Manager Forum") miteinander verbunden. An ihren Telefonkonferenzen nehmen die Settlement-Manager der Zentralbanken, die SSP-Service-Manager und der TARGET2-Koordinator teil.

Jede Zentralbank hat darüber hinaus einen **Krisenmanager**, der vom jeweiligen Settlement-Manager informiert und bei Eskalation eines Problems hinzugezogen wird. Die Krisenmanager sind ebenfalls über ein voreingestelltes Telekonferenzsystem miteinander verbunden. An den Telefonkonferenzen der TARGET2-Krisenmanager nehmen die ZB-Krisenmanager, die SSP-Krisenmanager und die EZB-Krisenmanager teil.

Die Settlement-Manager und die Krisenmanager der einzelnen Zentralbanken nehmen auch an den entsprechenden T2S-Telefonkonferenzen teil

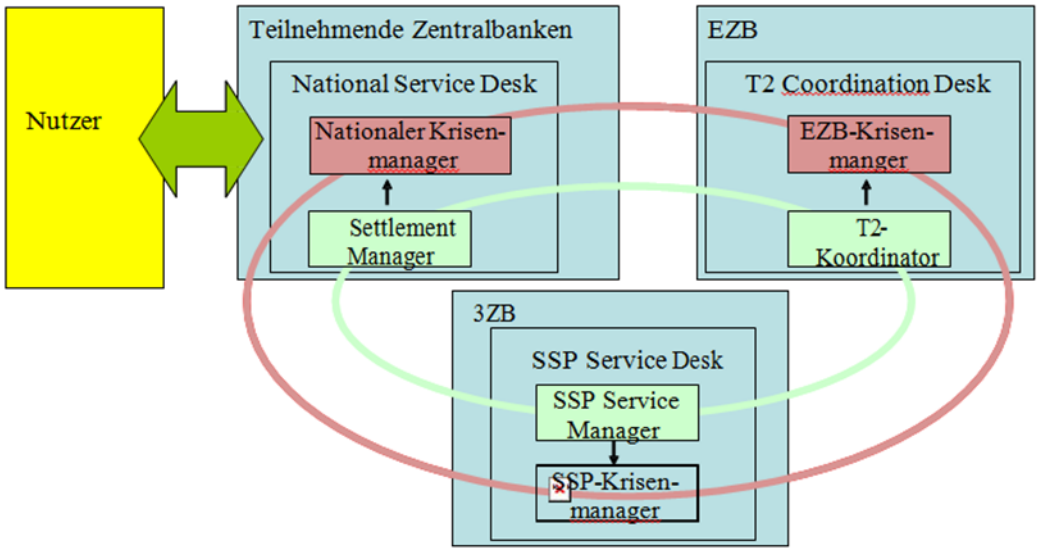


Abbildung 3: Überblick über die TARGET2-Beteiligten

2.4 Kommunikation mit den Nutzern

Ansprechpartner für TARGET2-Nutzer ist der National Service Desk. Dabei gilt jedoch:

a) Bei Konnektivitätsproblemen kann ein Geldkontoinhaber mit direkter T2S-Anbindung den T2S Service Desk direkt kontaktieren. Dieser eröffnet ein Ticket und informiert die entsprechende Zentralbank. Bei Zweifeln darüber, ob es sich um ein Konnektivitätsproblem handelt, sollte der direkt angeschlossene Geldkontoinhaber den National Service Desk kontaktieren. Kontaktaufnahmen zum T2S Service Desk, die nichts mit Konnektivitätsfragen zu tun haben, sollten an die National Service Desks weitergeleitet werden (und umgekehrt). Die direkt angebundenen Geldkontoinhaber erhalten die Kontaktdaten des T2S Service Desk über die entsprechende Zentralbank.

b) Bei Konnektivitätsfragen kann der T2S Service Desk unmittelbar angeschlossene DCA-Inhaber auch direkt kontaktieren, wovon er den National Service Desk in Kenntnis setzt. Die Kontaktdaten der Person bzw. des Teams, die/das für Fragen zur T2S-Konnektivität der jeweiligen direkt angebundenen Geldkontoinhaber verantwortlich ist, werden von der jeweiligen Zentralbank eingeholt. Möchte ein Geldkontoinhaber nicht direkt vom T2S Service Desk kontaktiert werden, wird stattdessen Verbindung zum National Service Desk der Zentralbank aufgenommen (und dessen Kontaktdaten werden eingeholt).

2.4.1 Kommunikationsmittel

Folgende Kommunikationsmittel können zwischen der jeweiligen Zentralbank und ihren Nutzern verwendet werden:

Informations- und Steuerungsmodul (ICM)

Das Informations- und Steuerungsmodul (Information and Control Module – ICM) verschafft PM-Kontoinhabern und Nebensystemen Zugang zu einem breitgefächerten Spektrum allgemeiner Informationen wie z. B. Guthaben oder Transaktionen. Es ermöglicht den National Service Desks darüber hinaus, Nachrichten an ihre jeweilige nationale Bankengemeinschaft (außer an Geldkontoinhaber) zu senden. Ein Nachrichtenticker im oberen Teil des Bildschirms eignet sich ferner zur Versendung wichtiger Informationen. Nutzbar sind diese Tools nur, wenn ein ICM-Zugang verfügbar ist. Daher sind sie bei Konnektivitätsproblemen von SWIFTNet oder einem Ausfall der Gemeinschaftsplattform unter Umständen nicht verwendbar.

T2S GUI

T2S GUI ermöglicht direkt angeschlossenen Geldkontoinhabern zur Überwachung und Steuerung ihres Geschäfts (z. B. für die Verwaltung von Limiten) den Zugriff auf ein breites Spektrum

allgemeiner Informationen (z. B. über Kontostände oder Transaktionen). Darüber hinaus gestattet es den National Service Desks die Versendung von Nachrichten an ihre jeweiligen DCA-Inhaber.

Lokale Kommunikationsinstrumente (local tools)

Mit lokalen Tools sind nationale Kommunikationsmittel gemeint. Die zuständige NZB informiert ihre TARGET2-Nutzer über die zur Verfügung stehenden nationalen Kommunikationskanäle. Abrufbar sind die Kontaktangaben für die einzelnen Länder neben sonstigen länderbezogenen Informationen unter „Contact Items“ im ICM.

TARGET2-Informationssystem

Das TARGET2-Informationssystem (T2IS)[8] liefert aktuelle Informationen über den Betriebsstatus des TARGET2-Systems. Genutzt wird es von Nachrichtenagenturen, um Informationen über das TARGET2-System zu erhalten und an Dritte, z. B. Geldmarkthändler oder die Medien, weiterzugeben. Das T2IS ist auch über die Website der EZB zugänglich.

Sollte TARGET2 einmal nicht voll funktionsfähig sein, werden Informationen über die Art des Ausfalls, seine Auswirkungen und die zur Problemlösung ins Auge gefassten Maßnahmen per T2IS bekannt gegeben.

T2S-Informationssystem

Das T2S-Informationssystem (T2S-IS) liefert aktuelle Informationen zum Betriebsstatus des Systems für die T2S-Dienstleistungen an Dritte. T2S-IS informiert sowohl über normale Betriebsabläufe als auch über Ausnahmesituationen. In letzterem Fall werden Informationen über die Art des Ausfalls, seine Auswirkungen und die zur Problemlösung ins Auge gefassten Maßnahmen per T2S-IS bekannt gegeben.

[8] Ähnlich wie bei TARGET2 wird ein T2S-Infosystem aufgebaut.

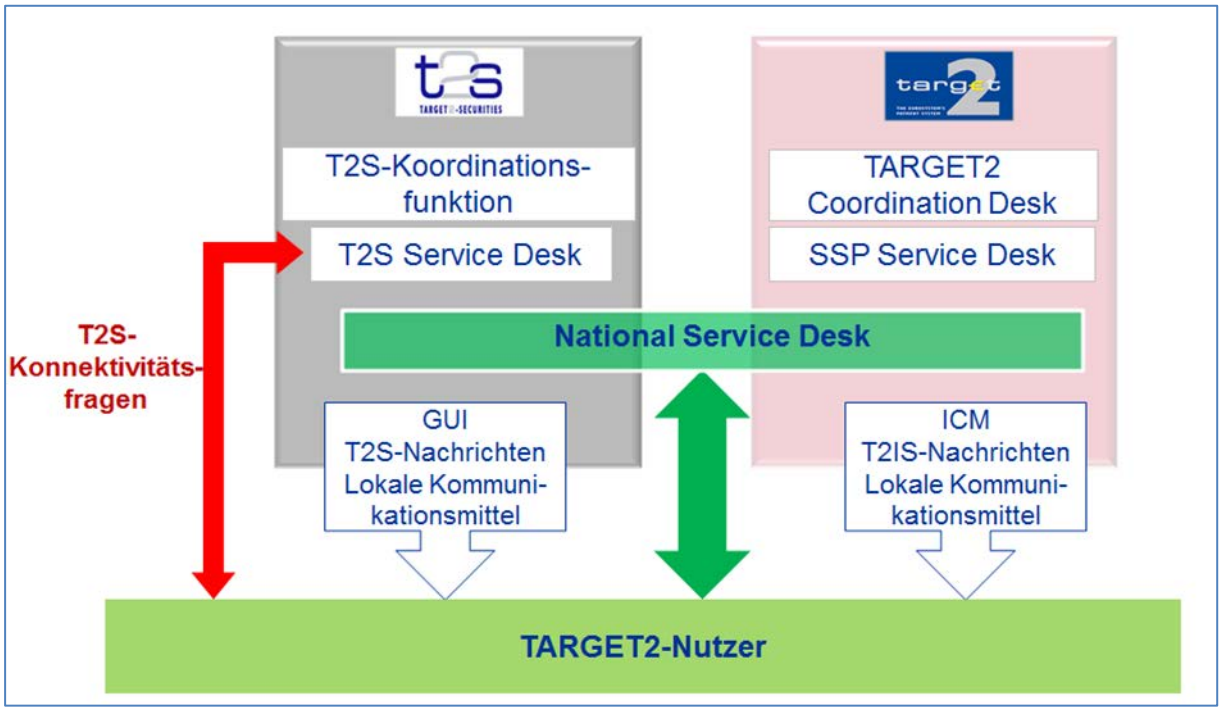


Abbildung 4: Informationsfluss

2.5 Öffnungstage

Die TARGET2-Öffnungstage sind de facto die Abwicklungstage für die Euro-Finanzmärkte sowie für Devisentransaktionen mit dem Euro als Währung.

Geöffnet ist TARGET2 täglich außer samstags, sonntags, Neujahr, Karfreitag und Ostermontag (nach dem am Sitz der EZB gültigen Kalender) und außer dem 1. Mai und dem 25. und 26. Dezember. Derselbe Kalender gilt für die T2S-Geldverrechnung in Euro.

Zwar steht T2S am 1. Mai, dem Karfreitag sowie dem Ostermontag zur Verfügung, doch es erfolgt keine Abwicklung in Euro – lediglich Free-of-payment-Transaktionen sind möglich. Das heißt, dass es an diesen Feiertagen zu einer Zeitlücke zwischen dem Moment kommt, in dem Daueraufträge zu Liquiditätsübertragungen von PM-Konten auf Geldkonten auf der Gemeinschaftsplattform und auf der T2S-Plattform verarbeitet werden. Die Verarbeitung auf der Gemeinschaftsplattform erfolgt um 19.30 Uhr am Vorabend des 1. Mai und der Osterfeiertage für den nächsten TARGET2-Geschäftstag, der auf den Tag nach dem 1. Mai bzw. der Osterfeiertage fällt. Auf der T2S-Plattform erfolgt sie um 20.00 Uhr am Abend des 1. Mai und der Osterfeiertage, wenn der T2S-Geschäftstag beginnt, der dasselbe Wertstellungsdatum trägt wie in TARGET2. Anders formuliert, die Daueraufträge zu Liquiditätsübertragungen müssen auf die T2S-Abwicklung nicht 30 Minuten, sondern mindestens 24 Stunden und 30 Minuten warten.

Abbildung 5: TARGET2 und T2S-Feiertage

2.6 Tagesablauf

Nachstehende Tabelle präsentiert die verschiedenen Phasen eines TARGET2- und T2S-Geschäftstags.

SSP-Zeitplan		**T2S-Zeitplan (gilt für Geldkonten)**	
Zeit	**Beschreibung**	**Zeit**	**Beschreibung**
18.45 Uhr – 19.00 Uhr(1)	Tagesbeginn-Verarbeitung (2)	18.45 Uhr – 20:00 Uhr	Tagesbeginn - Umstellung des Geschäftsdatums - Annahmeschluss für Datenaktualisierungen im Zusammenhang mit der Client Auto-Collateralisation (19.00 Uhr) - Vorbereitung der Nachtverarbeitung
19.00 Uhr – 19.30 Uhr(1) 19.30 Uhr(1) – 22.00 Uhr	Nachtverarbeitung (NTS1): Liquiditätsbereitstellung von SF nach HAM und PM sowie von HAM und PHA nach PM. Nachtverarbeitung (NTS1): Nachricht „Beginn des Verfahrens" Bereitstellung von Liquidität auf Basis der Daueraufträge für die Nachtverarbeitung (Nebensysteme: AS-Abwicklungsverfahren 6 und T2S)	20.00 Uhr – 03.00 Uhr	Nachtverarbeitung: - Erster Nachtverarbeitungszyklus - Letzter Nachtverarbeitungszyklus (Sequenz X umfasst die Teilabwicklung nicht abgewickelter Zahlungsaufträge, die für die Teilabwicklung zugelassen sind und die wegen fehlender Wertpapiere nicht abgewickelt wurden; Sequenz Y beinhaltet die Rückführung an Mehrfach-Liquiditätsanbieter am Ende des Zyklus)
22.00 Uhr – 1.00 Uhr	Technisches Wartungsfenster(3)	03.00 Uhr – 05.00 Uhr	Technisches Wartungsfenster(4)
1.00 Uhr – 06.45 Uhr	Nachtverarbeitung (Nebensysteme: AS-Abwicklungsverfahren 6 und T2S)		Tageshandel/Echtzeit-Abwicklung(5): - Vorbereitung der Echtzeit-Abwicklung(5) - Fenster für Teilabwicklungen um 14.00 Uhr und 15.45 Uhr[9] (für 15 Minuten)

[9] Jedes partielle Abwicklungsfenster ist für 15 Minuten geöffnet. Die partielle Abwicklung gilt für nicht abgewickelte

06.45 Uhr – 07.00 Uhr 07.00 Uhr – 18:00 Uhr	Betriebsfenster zur Vorbereitung des Tagesgeschäfts Tagverarbeitung - 17.00 Uhr: Annahmeschluss für Kundenzahlungen - 17.45 Uhr: Annahmeschluss für Liquiditätsüberträge auf Geldkonten - 18.00 Uhr: Annahmeschluss für Interbankzahlungen und eingehende Liquiditätsüberträge von Geldkonten	05.00 Uhr – 18.00 Uhr	- 16.00 Uhr DvP-Annahmeschluss /Annahmeschluss für die Rückführung der Selbstbesicherung durch Payment Banks - 16.30 Uhr Automatisierte Rückführung der Selbstbesicherung und anschließender optionaler „Cash Sweep" - 17.40 Uhr: Annahmeschluss für bilaterale Geldhandelsgeschäfter (Bilaterally Agreed Treasury Management – BATM) und für Zentralbankgeschäfte (Central Bank Operations – CBO) 17.45 Uhr: Annahmeschluss für eingehende Liquiditätstransfers Automatischer Cash Sweep (Abschöpfung der Guthaben) nach 17.45 Uhr 18.00 Uhr: FOP-Annahmeschluss
18.00 Uhr – 18:45 Uhr	- 18.15 Uhr(1): Annahmeschluss für die Inanspruchnahme ständiger Fazilitäten - 18.30 Uhr(1): Zentralbankverbuchung Tagesendeverarbeitung	18.00 Uhr – 18:45 Uhr	- Verarbeitungsende der T2S-Abwicklung - Recycling und Bereinigung - Tagesaend-Berichte und Kontoauszüge

Tabelle 2: Zeitplan an einem Geschäftstag

(1) Beginnt/endet am letzten Tag der Mindestreserve-Erfüllungsperiode 15 Minuten später.

(2) In der TARGET2-Leitlinie dauert die Tagesbeginn-Verarbeitung bis 19.30 Uhr (d. h. einschließlich der nachfolgenden Liquiditätsbereitstellung von 19.00 Uhr bis 19.30 Uhr), da sie aus geschäftlicher Perspektive eigentlich als Vorbereitung für die Zahlungsverarbeitung gilt.

(3) An Wochenenden oder Feiertagen bleibt das technische TARGET2-Fenster über das ganze Wochenende oder den ganzen Feiertag geöffnet, d. h., von Freitag 22.00 Uhr bis Montag 1.00 Uhr bzw. von 22.00 Uhr des letzten Geschäftstags vor dem Feiertag bis 1.00 Uhr des nächstfolgenden Geschäftstags.

Abwicklungsanweisungen, die für die partielle Abwicklung infrage kommen und mangels Wertpapieren nicht abgewickelt werden konnten.

(4) An Wochenenden oder Feiertagen bleibt das technische T2S-Fenster über das gesamte Wochenende oder den ganzen Feiertag geöffnet, d. h. von Samstag 3.00 Uhr bis Montag 5.00 Uhr bzw. von 3.00 Uhr am Feiertag bis 5.00 Uhr des nächstfolgenden Geschäftstags.

(5) Die Vorbereitung der Echtzeitabwicklung und die Echtzeitabwicklung können bereits vor dem Wartungsfenster beginnen, sofern der letzte Nachtverarbeitungszyklus vor 3.00 Uhr endet.

2.7 Transaktionen über TARGET2

Folgende Arten von Transaktionen werden in TARGET2 abgewickelt:

a) **Kundenzahlungen**

Kundenzahlungen werden über PM-Konten abgewickelt und sind als Zahlungen im Format SWIFT FIN MT103 definiert (Standard oder STP). Kundenzahlungen können über TARGET2 zwischen 7.00 Uhr und 17.00 Uhr verarbeitet werden.

b) **Interbankzahlungen**

Interbankzahlungen werden über die PM-Konten abgewickelt und als Zahlungsnachrichten im Format SWIFTNet FIN MT202 und MT202COV definiert. Diese Nachrichten werden vom oder im Namen des anweisenden Instituts an das Finanzinstitut des begünstigen Instituts – entweder direkt oder über einen Korrespondenten – übermittelt.

Interbankzahlungen, die über MT202 verarbeitet werden, sind Zahlungen wie die geldliche Verrechnung am Geldmarkt oder Devisen- und Derivatetransaktionen, die zwischen Kreditinstituten oder zwischen Zentralbanken und Kreditinstituten erfolgen. MT202COV sind Interbankzahlungen, die ihnen zugrunde liegende Kundenzahlungen „decken“ und Felder für den Auftraggeber und den Empfänger der Überweisung enthalten. Interbankzahlungen können über TARGET2 von 7.00 Uhr bis 18:00 Uhr verarbeitet werden.

c) **Lastschriften**

Lastschriften werden über die PM-Konten abgewickelt und sind als Zahlungsnachrichten im Format SWIFTNet FIN MT204 definiert. Lastschriften in TARGET2 sind Transaktionen zwischen Banken, die ausschließlich für Großeinreicher vorgesehen sind. Die betreffenden PM-Kontoinhaber müssen mit den Parteien, die eine Belastung ihrer Konten gestatten, die Bedingungen für die Inanspruchnahme dieser Dienstleistung vereinbaren. Der Inhaber des PM-Kontos gestattet es einem anderen PM-Kontoinhaber, eine Lastschrift einzureichen, und informiert seine Zentralbank, die für die Erfassung und Verwaltung der getroffenen Vereinbarungen zuständig ist, entsprechend. Lastschriften können über TARGET2 zwischen 7.00 Uhr und 18.00 Uhr verarbeitet werden. Inhaber von PM-Konten, die einen internetbasierten Zugang nutzen, können keine Lastschriftanweisungen ausstellen (sie aber entgegennehmen).

d) **Nebensystem-Transaktionen**

Zahlungen im Zusammenhang mit der Abwicklung von Nebensystemen: Massenzahlungssysteme, Großbetragszahlungssysteme, Devisenhandelssysteme, Geldmarkthandelssysteme, Clearinghäuser und Wertpapierabwicklungssysteme.

e) **Liquiditätsübertragungen**

Liquidität in Zentralbankgeld kann auf PM-Konten, Heimatkonten oder Geldkonten gehalten werden, wobei die Möglichkeit des Liquiditätstransfers zwischen den verschiedenen Konten besteht.

Liquiditätsübertragungen im Zusammenhang mit PM-Konten (aber nicht Geldkonten) können über SWIFTNet FIN MT 202 von 7.00 Uhr bis 18.00 Uhr oder über ICM (im U2A- oder A2A-Modus) auf der Basis von SWIFTNet InterAct ausgeführt werden. Mittels ICM veranlasste Liquiditätstransfers werden während der Betriebszeiten des Zahlungsmoduls bis zum Annahmeschluss für Interbankzahlungen (18.00 Uhr) und ab dem Beginn der Nachtverarbeitung (19.30 Uhr) – mit Ausnahme spezieller Zeitfenster zur Wartung der Gemeinschaftsplattform – sofort nach der Übermittlung ausgeführt.[10]

Informationen zu Liquiditätsübertragungen von PM-Konten auf Geldkonten und umgekehrt sowie zu Liquiditätstransfers zwischen Geldkonten (die derselben Payment Bank gehören oder mit demselben PM-Hauptkonto verlinkt sind) stehen in Abschnitt 2.8 zur Verfügung.

f) **Geldliche Verrechnung von Wertpapiertransaktionen**, die auf Geldkonten abgewickelt werden:
   - Lieferung gegen Zahlung (Delievery versus Payment – DVP) und Erhalt gegen Zahlung (Receive versus Payment – RVP), definiert als Tausch von Wertpapieren gegen Zahlung;
   - - Lieferung mit Gegenwertverrechnung (Delivery with Payment – DWP), definiert als Wertpapierlieferung von einer zur anderen Partei bei gleichzeitig erfolgender Zahlung;
   - Gegenwertverrechnung ohne Lieferung (Payment Free of Delivery – PFOD), die den Tausch von Geld ohne die Lieferung von Wertpapieren darstellen;
   - Abwicklungsrestriktionen, die die Blockierung und Reservierung von Geld in einem Geldkonto ermöglichen.

Es sei angemerkt, dass T2S auch FoP-Transaktionen (Free of Payment) verarbeitet, in denen Wertpapiere geliefert (Delivery Free of Payment – DFOP) oder empfangen (Receive Free of Payment

[10] Zu den Verarbeitungszeiten bei Daueraufträgen vgl. UDFS-Buch 1.

– RFOP) werden können, ohne dass eine Gegenwertverrechnung erfolgt. Definitionsgemäß erfordert diese Transaktionsart allerdings keine Geldbewegungen und wird daher nicht auf der Basis von Geldkonten abgewickelt.

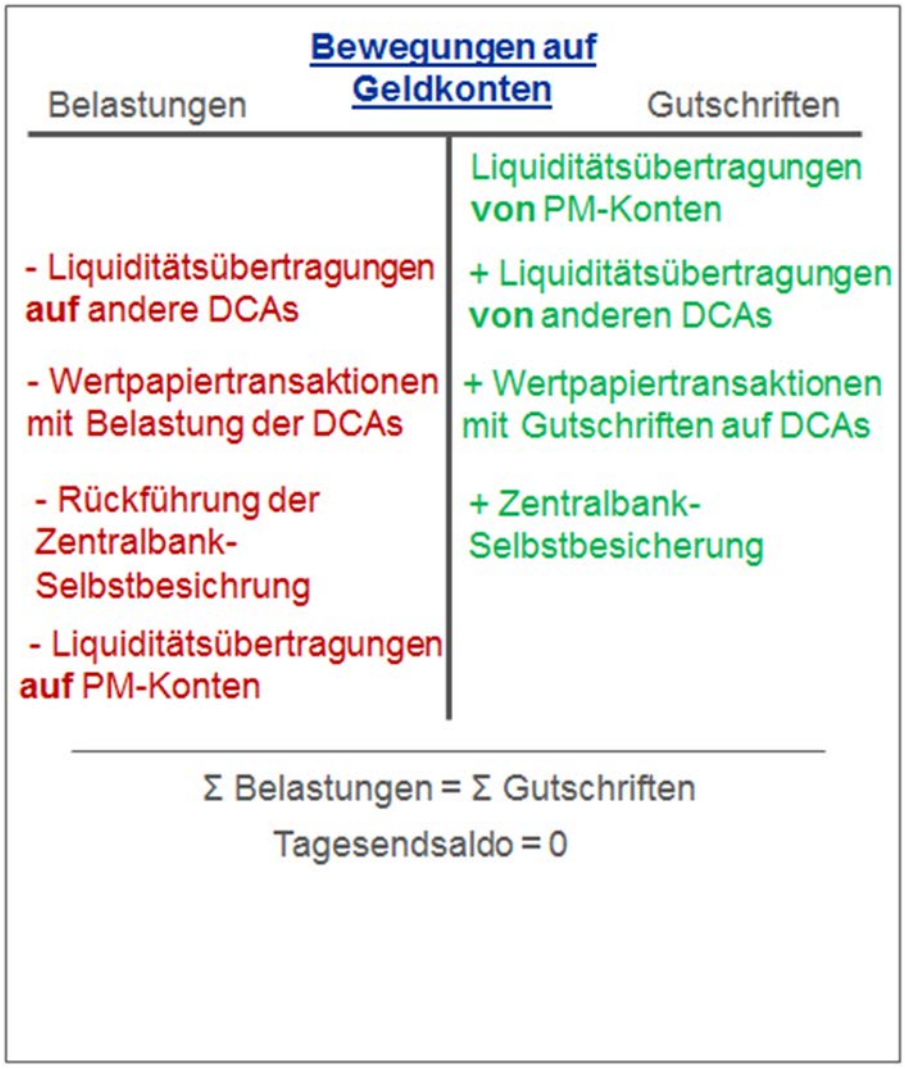


Abbildung 6: Bewegungen auf Geldkonten

2.8 Liquiditätsströme zwischen PM-Konten und Geldkonten sowie zwischen Geldkonten

Es ist möglich, Liquidität von PM-Konten auf Geldkonten und von Geldkonten auf PM-Konten zu transferieren. Daneben ist es möglich, Liquidität zwischen Geldkonten zu übertragen, wenn die beteiligten DCAs mit demselben RTGS-Konto verlinkt sind oder demselben Geldkontoinhaber gehören.

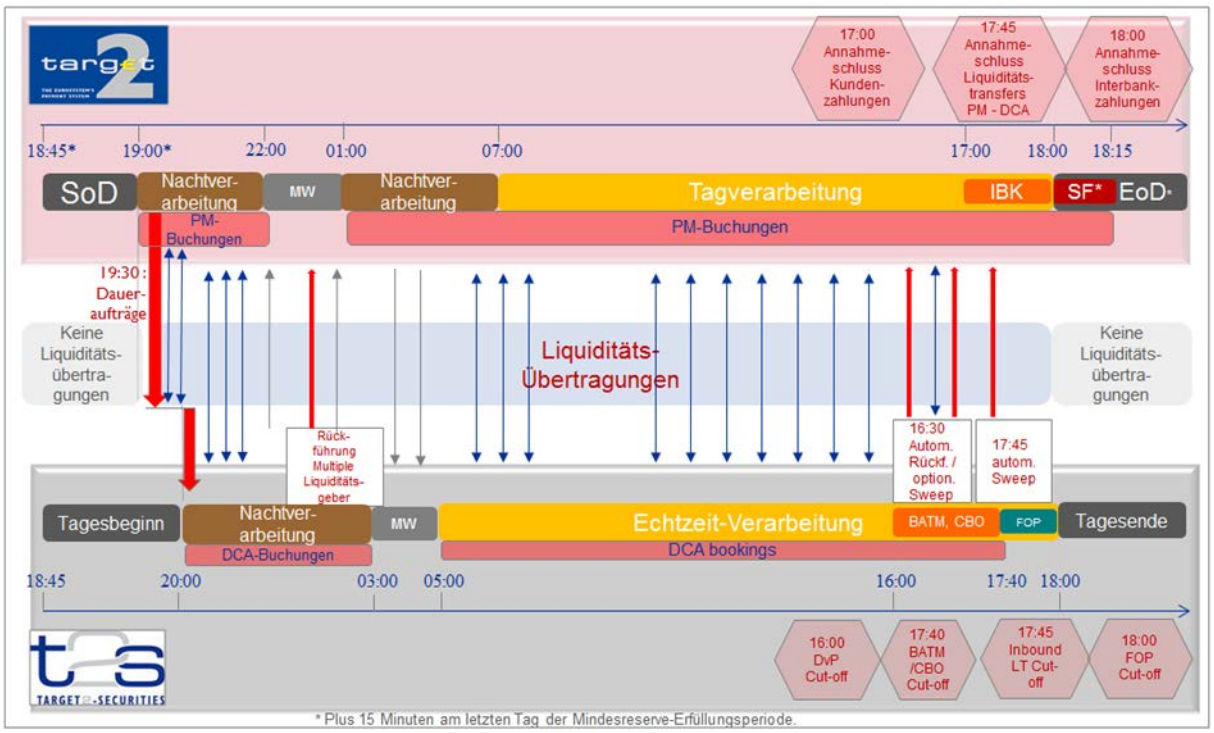


Abbildung 7: Liquiditätsströme zwischen PM-Konten und Geldkonten

Liquiditätsübertragungen zwischen Geldkonten sind nur dann möglich, wenn die DCAs mit demselben RTGS-Konto verlinkt sind oder demselben Geldkontoinhaber gehören. Diese Liquiditätstransfers können in T2S ab dem ersten Nachtverarbeitungszyklus – Sequenz 0 abgewickelt werden (siehe Abschnitt 4.4). Eine Teilausführung bei ungenügender Liquidität auf dem DCA ist lediglich dann möglich, wenn der Liquiditätstransfer von einer dritten Partei veranlasst wird, die vom Geldkontoinhaber dazu autorisiert wurde.

Bei **Liquiditätsübertragungen von PM-Konten auf Geldkonten** lässt sich zwischen folgenden Aufträgen unterscheiden:

a) **Daueraufträge**, die vom Inhaber eines PM-Kontos eingerichtet wurden

Auf der Gemeinschaftsplattform wird ein Dauerauftrag regelmäßig in der angegebenen Höhe ausgeführt, bis er geändert wird. Die Aufträge können bis spätestens 18.00 Uhr (wirksam mit der nächsten Nachtverarbeitung) eingestellt werden. Die Ausführung auf der Gemeinschaftsplattform erfolgt unmittelbar nach der automatischen Durchgabe der Nachricht „Beginn des Verfahrens" („Start-of- procedure") (nur bei der Nachtverarbeitung) bzw. auf der T2S-Plattform während der Sequenz 0 des ersten Nachtverarbeitungszyklus. Bei ungenügender Liquidität auf dem PM-Konto

erfolgt die Teilausführung aller zu diesem Zeitpunkt anstehenden Daueraufträge (d. h. zusammen mit den ASI-Daueraufträgen); siehe Abschnitt 4.3 (Konkordanz von Aufträgen).

b) **Laufende Aufträge**, die vom Inhaber eines PM-Kontos generiert wurden

Der Auftrag kann im Push-Modus (über die TARGET2-Standardleistungen) oder im Pull-Modus erfasst werden, wenn der PM-Kontoinhaber die TARGET2-Zusatzleistungen für T2S verwendet. Die laufenden Aufträge, die von einem PM-Kontoinhaber initiiert wurden, werden zurückgewiesen, falls die Liquidität nicht ausreicht (keine Teilausführung).

Auf der T2S-Plattform eingegangene laufende Aufträge können ab dem ersten Nachtverarbeitungszyklus, Sequenz 0 abgewickelt werden. Die Ausführung erfolgt sofort, wenn die Nachtverarbeitung begonnen hat und sie zwischen zwei Sequenzen eingehen. Werden sie während der Verarbeitung einer Sequenz entgegengenommen, so erfolgt die Abwicklung mit der nächstfolgenden Sequenz.

c) **Laufende Aufträge** einer dritten Partei (T2S-Beteiligter in TARGET2),[11] die im Auftrag des PM-Kontoinhabers handelt

Die Hinterlegung eines laufenden Auftrags durch einen Dritten für den PM-Konteninhaber beruht auf internationalen Regeln. Diese Aufträge werden sofort ausgeführt, sobald sie abgesandt und die T2S-Nachtverarbeitung begonnen hat. Bei ungenügender Liquidität erfolgt lediglich eine Teilausführung.

Bei der **Liquiditätsübertragung von Geld- auf PM-Konten** unterscheidet man zwischen folgenden Varianten:

a) **sofortiger Liquiditätstransfer**, der auf der T2S-Plattform initiiert wird

Sofortige, auf der T2S-Plattform ausgelöste Liquiditätsübertragungen werden während der Nachtverarbeitung ab dem ersten Zyklus, Sequenz 1 unmittelbar ausgeführt. Gehen sie während der Verarbeitung einer Sequenz ein, werden sie gespeichert. Eine Teilausführung bei ungenügender Liquidität auf dem DCA ist lediglich dann möglich, wenn der Liquiditätstransfer von einer dritten Partei veranlasst wird, die vom Geldkontoinhaber dazu autorisiert wurde. Bei sofortigen Liquiditätstransfers, die vom Geldkontoinhaber selbst veranlasst wurden, erfolgt bei mangelnder Liquidität keine Teilausführung, sondern sie werden zurückgewiesen.

[11] Der Zugang als T2S-Beteiligter in TARGET2 ist eine spezielle Zugangsart zu TARGET2, die nur über T2SI und im A2A-Modus erfolgen kann, worüber eine dritte Partei (wie zum Beispiel ein Zentralverwahrer) laufende Aufträge zum Liquiditätstransfer auf T2S im Namen eines PM-Kontoinhabers generieren kann.

b) **Vorab auf der T2S-Plattform erstellter Liquiditätstransferauftrag**

Ein vorab festgelegter Liquiditätsauftrag wird nur einmal ausgeführt. Er kann durch ein Ereignis ausgelöst werden oder an einem bestimmten Zeitpunkt erfolgen. Es ist zulässig, mehr als einen vorab erstellten Auftrag für unterschiedliche Zeiten oder Ereignisse einzureichen. Der Auftrag kann auf einen bestimmten Teilbetrag oder den gesamten Saldo auf dem Geldkonto lauten. Bei ungenügender Liquidität werden vorab festgelegte Liquiditätstransferaufträge teilausgeführt; für den restlichen Teil, der beim ersten Versuch nicht ausgeführt werden konnte, erfolgt keine weitere Abwicklung.

c) **Dauerauftrag zur Liquiditätsübertragung**, der auf der T2S-Plattform initiiert wurde

In T2S lässt sich bei den Stammdaten ein Dauerauftrag erfassen. Dieser wird regelmäßig bis zu dessen Löschung ausgeführt. Auslöser für den Auftrag kann ein bestimmtes Ereignis oder ein bestimmter Zeitpunkt sein. Der Auftrag kann auf eine bestimmte Summe oder den gesamten Saldo auf dem Geldkonto lauten. Es ist möglich, während des Geschäftstages verschiedene Aufträge für unterschiedliche Zeiten oder Ereignisse zu erfassen. Bei mangelnder Liquidität erfolgt eine Teilausführung.

Art der Liquiditätsübertragung		**Teilausführung**	**Periodizität**	**Ausführungszeiten**
Von PM- auf Geldkonten	Dauerauftrag	ja	jeder Geschäftstag	Tagesbeginn
	laufender Auftrag	nein	einmalig	Bei Anweisung
	laufender Auftrag durch eine Drittpartei (T2S-Akteur in TARGET2)	ja	einmalig	bei Anweisung
Von Geld- zu PM-Konten	sofortiger Liquiditätstransfer	ja	einmalig	bei Anweisung
	vorab festgelegter Liquiditätstransferauftrag	ja	einmalig	vorab festgelegter Zeitpunkt/vorab festgelegtes Ereignis
	Dauerauftrag zur Liquiditätsübertragung	ja	jeder Geschäftstag	vorab festgelegter Zeitpunkt/vorab festgelegtes Ereignis
Zwischen verschiedenen Geldkonten	Interne und sofortige Liquiditätsübertragung	nur bei Anweisung durch eine Drittpartei	einmalig	bei Anweisung

Tabelle 3: Liquiditätsüberträge - Überblick

Kasten 1: Euro-Zwischenkonten

Es gibt zwei Euro-Zwischenkonten für die Abwicklung und das Monitoring aller Liquiditätstransfers zwischen der SSP und der T2S-Plattform, d. h. zwischen den PM-Konten und den Geldkonten. Die Liquiditätsströme einschließlich Zwischenkonten sind im folgenden Schaubild dargestellt:

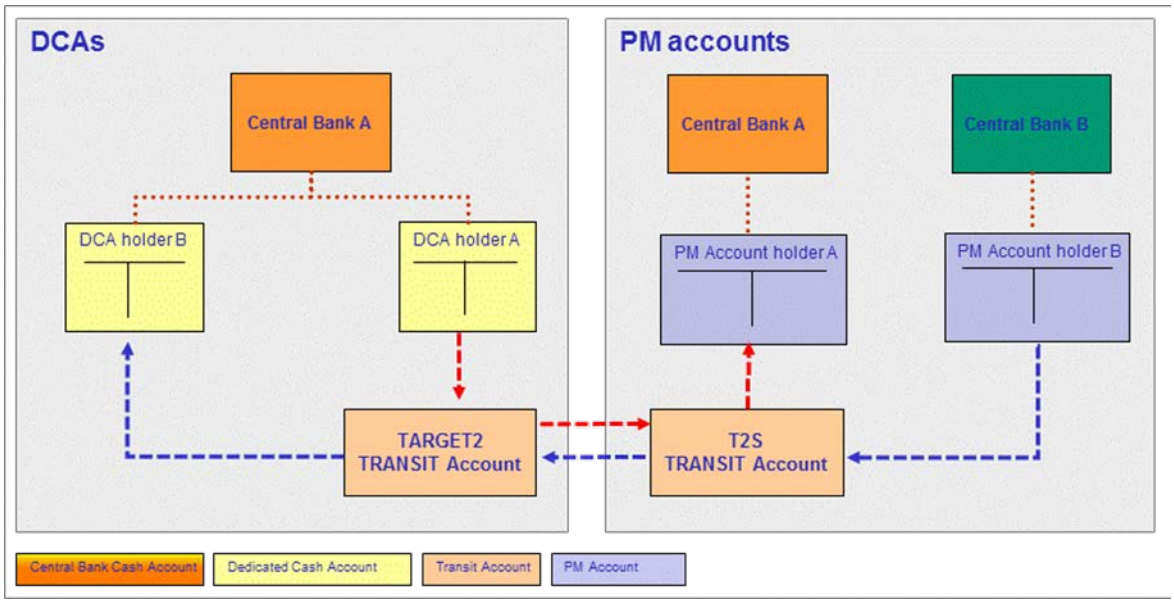


Abbildung 8 Euro-Zwischenkonten

Wie vorstehend illustriert, gibt es ein TARGET2-Zwischenkonto auf der T2S-Plattform (das alle Bewegungen abbildet, die sich auf die Geldkonten auswirken) und ein T2S-Zwischenkonto auf der SSP (das alle Bewegungen abbildet, die sich auf die PM-Konten auswirken). Die beiden Zwischenkonten haben Spiegelsalden und die Gesamtforderungen und Gesamtverbindlichkeiten ergeben bei Summierung null. Am Tagesende werden die Salden auf beiden Konten auf null reduziert (Gesamtverbindlichkeiten = Gesamtforderungen), da die Geldkonten über Nacht keine Salden aufweisen dürfen. Zu diesem Zweck werden alle anstehenden Selbstbesicherungen automatisch um 16.30 Uhr zurückgeführt und alle noch verbleibenden Guthaben auf den Geldkonten über das automatische „Cash Sweep" auf ihre entsprechenden PM-Hauptkonten transferiert; dies findet nach dem Annahmeschluss für eingehende Liquiditätsübertragungen um 17.45 Uhr statt.

2.8.1 Initiierung von Liquiditätstransfers

Inhaber von Geldkonten, die direkt an T2S angebunden sind, können Liquiditätsübertragungen in T2S im A2A-Modus mittels ISO20022-Nachrichten oder im U2A-Modus via T2S GUI veranlassen.

Indirekt an T2S angebundene Geldkontoinhaber, die die TARGET2-Zusatzleistungen für T2S [12] nutzen, können Liquiditätsübertragungen von dem T2S-Geldkonto auf das PM-Konto mithilfe von ICM, MT202-Nachrichten oder einer LiquidityCreditTransfer-Nachricht ohne Business Application Header (BAH) vornehmen und auch die Salden auf den jeweiligen Geldkonten einsehen.

Liquiditätstransfers von Geldkonten (die direkt in T2S oder über TARGET2 VAS für T2S veranlasst wurden) werden auf der Gemeinschaftsplattform durchgehend außer während der Tagesende- und Tagesbeginn-Verarbeitung (kurz nach 18.00 Uhr bis 19.30 Uhr) und auch nicht während des technischen Wartungsfensters (22.00 Uhr bis 1.00 Uhr) verarbeitet. Da der Saldo auf den Geldkonten am Ende des Geschäftstages null betragen muss, müssen alle Liquiditätsübertragungen auf PM-Konten vor der Ausführung des letzten Algorithmus (kurz nach 18.00 Uhr) verarbeitet sein. Dies wird durch den „Automated Sweep” in T2S gegen 17.45 Uhr sichergestellt.

Liquiditätstransfers von PM-Konten auf Geldkonten sind in der SSP zu veranlassen und werden mit Beginn des neuen Geschäftstags von 19.30 Uhr (unterbrochen durch das Wartungsfenster von 22.00 Uhr bis 1.00 Uhr) bis zum Annahmeschluss für Liquiditätstransfers auf T2S (17.45 Uhr) durchgeführt. Alle PM-Kontoinhaber mit SWIFT-basiertem Zugang können Liquditititätsübertragungen auf Geldkonten vornehmen.

Nachfolgende Tabelle gewährt einen Überblick darüber, **wie die Liquidität zwischen PM-Konten und Geldkonten sowie zwischen DCAs bewegt werden kann**, d. h. entweder im U2A-Modus (über ICM oder T2S-GUI) oder im A2A-Modus:

[12] Nähere Information finden sich im UDFS-Buch 1.

Art der Liquiditäts-übertragung		User-to-Application (U2A)			Application-to-Application (A2A)		
		TARGET2-Standardleistungen (ICM)	**TARGET2 VAS (ICM) einschließlich Standardleistungen**	**T2S GUI**	**TARGET2-Standardleistungen**	**TARGET2 VAS, einschließlich Standardleistungen**	**T2S**
Von PM-auf Geldkonten	Dauerauftrag	✔	✔	–	✔	✔	–
	laufender Auftrag	✔	✔	–	✔[13]	✔[14]	–
	laufender Auftrag durch eine dritte Partei initiiert (T2S-Beteiligter in TARGET2)	–	–	-	✔[15]	✔[16]	-
Von Geldkonten auf PM-Konten	Sofortige Liquiditäts-übertragung	–	–	✔	-	-	✔
	Vorab festgelegter Auftrag zur Liquiditäts-übertragung	–	–	✔	-	-	✔
	Dauerauftrag	–	–	✔	-	-	✔
	laufender Auftrag	-	✔	-	-	✔[17]	-
Zwischen Geldkonten	Sofortige Liquiditäts-übertragung	–	–	✔	–	–	✔

Tabelle 4: Liquiditätsübertragung zwischen Geldkonten und PM-Konten

13 Möglich über XML-Nachricht.

14 Möglich über XML-Nachricht oder MT202.

15 Möglich über XML-Nachricht.

16 Möglich über XML-Nachricht oder MT202.

17 Möglich über XML-Nachricht oder MT202.

2.9 Nachrichtenfluss

In TARGET2 gibt es grundsätzlich zwei Arten von Nachrichten: SWIFTNet FIN-Nachrichten (insbesondere Kunden- und Interbankzahlungen sowie Lastschriften) und XML-Nachrichten (InterAct und FileAct).

SWIFT-FIN-Nachrichten

Das Zahlungsmodul (PM) der Gemeinschaftsplattform nutzt den SWIFTNet FIN Y-Copy-Service[18] zur Verarbeitung sämtlicher Zahlungen innerhalb einer eigens dafür eingerichteten SWIFT Closed User Group (CUG). Das Zahlungsmodul erhält eine vollständige Kopie jeder Zahlung, um die Abwicklung sowie eine effiziente und umfassende Informationsbereitstellung im Informations- und Steuerungsmodul (Information and Control Module - ICM) zu ermöglichen.

SWIFT-FIN-Nachrichten können bis zu fünf TARGET2-Geschäftstage im Voraus eingereicht werden. In diesem Fall wird die Zahlungsnachricht bis zur Tagesverarbeitung der Gemeinschaftsplattform gespeichert („warehoused payments“).

Nutzer, die über einen internetbasierten Zugang mit der Gemeinschaftsplattform verbunden sind, führen den Austausch von Nachrichten mit der SSP nicht über das SWIFT-Netzwerk durch, sondern sie können diese über ICM-Erfassungsmasken erfassen und anzeigen lassen. Eine Verbindung mit dem ICM für solche Nutzer ist nur im User-to-Application-Modus möglich (siehe auch 3.2. „Internetbasierter Zugang”).

[18] Im HAM wird V-Shape genutzt.

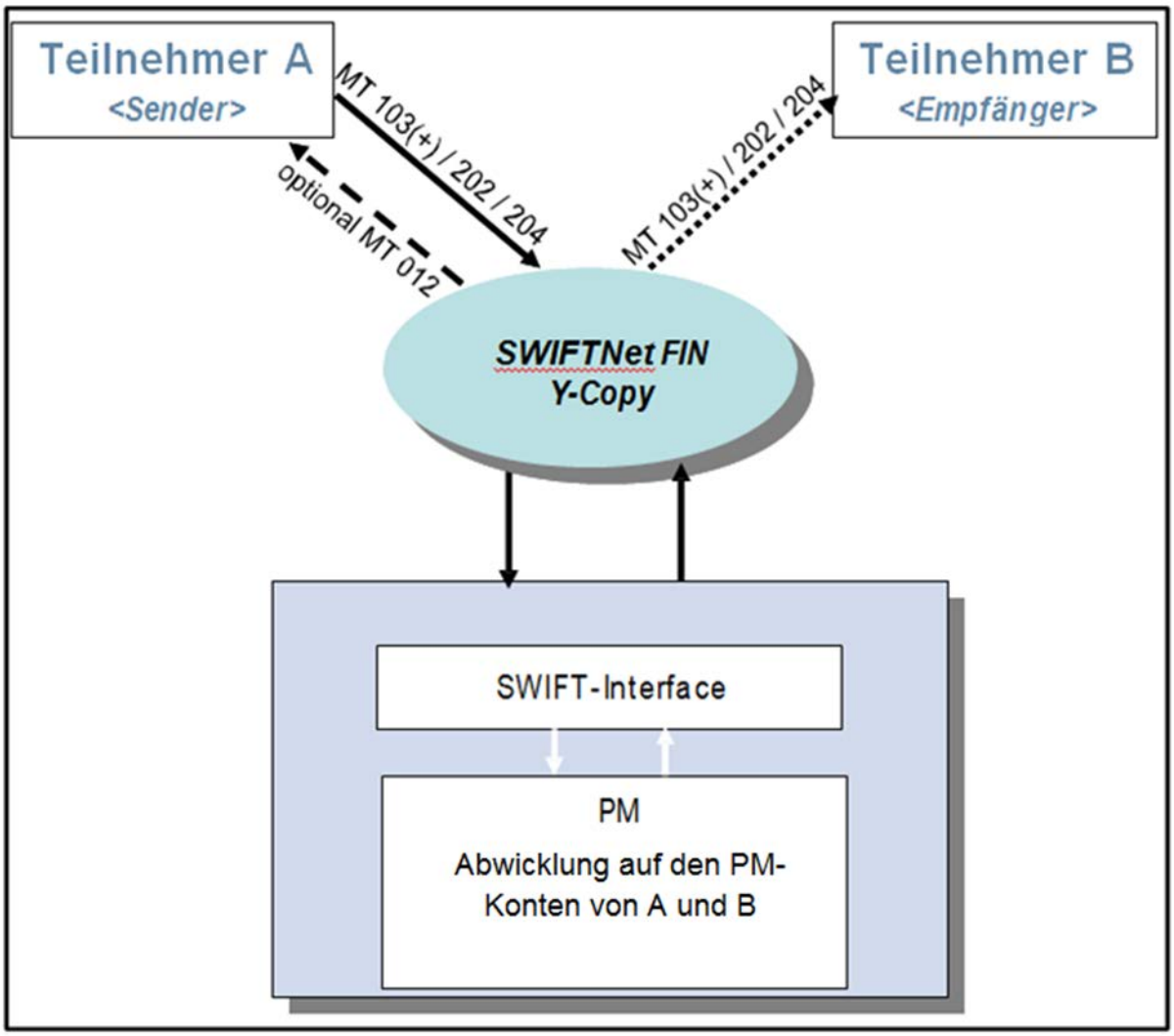


Abbildung 9: Transaktionsfluss in Y-Copy

In den TARGET2-UDFS Buch 1 (siehe 9.1.2.1.1.3 SWIFTNet FIN messages – User header – „Structure when sending a message“ bzw. „Structure when receiving a message“) wird das Feld-Kennzeichen 113 „Banking priority“ erläutert. Wie dort erklärt, bleiben die dritte und die vierte Stelle des Feldes 113 ungenutzt (und werden von der Gemeinschaftsplattform nicht geprüft). TARGET2-Nutzer sollten die nationalen Vereinbarungen zur Verwendung des Feld-Kennzeichens kennen.

XML-Nachrichten

Ist ein Teilnehmer mit dem ICM im „Application to Application“-Modus (A2A) verbunden, werden SWIFTNet InterAct und SWIFTNet FileAct genutzt. Die verschiedenen Informations- und

Kontrolloptionen sind als XML-Nachrichten konzipiert.[19]. SWIFTNet Browse ermöglicht die Initiierung eines InterAct- oder FileAct-Nachrichtenaustausches über eine sichere Browserverbindung.

SWIFTNet FileAct ermöglicht die Übermittlung von Dateien und wird in der Regel zum stapelweisen Austausch strukturierter Finanznachrichten und umfangreicher Berichte verwendet. SWIFTNet FileAct-Nachrichten werden während der Betriebszeiten des PM jederzeit angenommen, außer wenn die Gemeinschaftsplattform gewartet wird, während der Tagesende- und Tagesbeginn-Verarbeitung und auch nicht, wenn Liquidität bereitgestellt wird.

SWIFTNet InterAct ermöglicht die Übertragung von XML-Anfragen über das Secure IP Network (SIPN) durch SWIFT an das ICM und die Nebensystemschnittstelle (Ancillary System Interface – ASI). XML-Nachrichten werden für Anfragen und Antworten im Zusammenhang mit dem ICM (A2A-Modus) sowie für Geschäftsvorgänge der Nebensysteme genutzt. Die Nachrichten zu Geschäftsvorgängen der Nebensysteme werden wie in den TARGET2-UDFS Buch 1 erläutert angenommen. Bei ICM-(A2A-)Vorgängen werden die Nachrichten entsprechend dem zugrunde liegenden Geschäftsvorfall angenommen. Während des SSP-Wartungsfensters werden keine SWIFTNet InterAct-Nachrichten angenommen.

Die gemeinsame Systemschnittstelle von TARGET2 und T2S verwendet ebenfalls XML-Nachrichten, die gemäß T2S-Anforderungen im Einklang mit der ISO 20022-Norm stehen. XML-Nachrichten, die von TARGET2-Nutzern im Rahmen der TARGET2-Standard- und Zusatzleistungen für T2S verwendet werden, basieren ebenfalls auf demselben Standard, doch der Business Application Header ist nicht erforderlich. Direkt an T2S angebundene Geldkontoinhaber müssen auch den Nachrichtenstandard ISO 20022 gemäß den T2S-Anforderungen anwenden.

[19] Eine detaillierte Beschreibung der XML-Nachrichten findet sich im UDFS-Buch 4

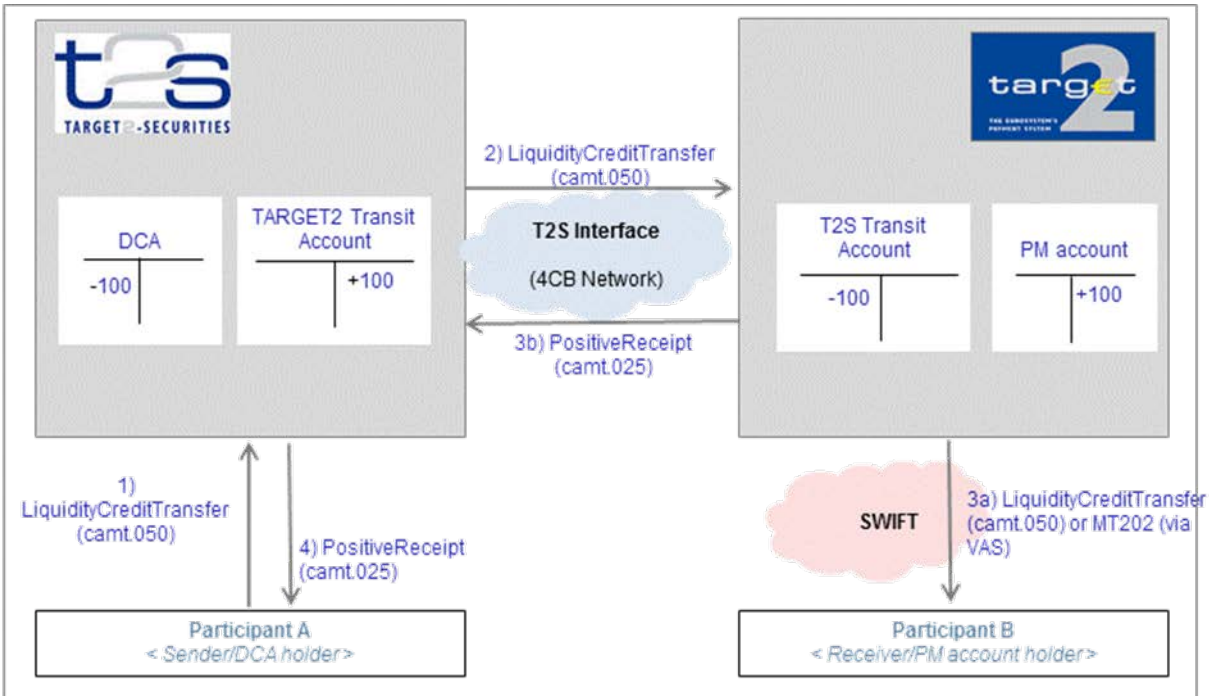


Abbildung 10: Liquiditätsübertragung von T2S auf TARGET2 (ISO 20022 Nachrichtenströme)

2.10 Abwicklung von Nebensystemen[20]

Nebensysteme können auf die Abwicklung innerhalb der SSP sowohl über die Standard-Teilnehmer-Schnittstelle (Participant Interface – PI) als auch über die Nebensystem-Schnittstelle (ASI) zugreifen. Im ersten Fall können Nebensysteme, die die Voraussetzungen für die Teilnahme als PM-Kontoinhaber erfüllen, die Systemfunktionalitäten wie jeder andere PM-Kontoinhaber nutzen. Insbesondere verfügen sie über ein PM-Konto auf der Plattform. Im zweiten Fall werden die Nebensysteme auf die Gemeinschaftsplattform über eine spezielle Schnittstelle (die ASI) zugreifen, die über eine Reihe spezifischer Merkmale verfügt, die eigens zur Ermöglichung der AS-Abwicklung konzipiert wurden, so z. B. die zentralisierte Steuerung der Autorisierung der Belastung eines bestimmten Kontos, die Nutzung von Mandated Payments, spezielle Abwicklungsverfahren, optionale Mechanismen und die Nutzung bestimmter Kontoarten (technische Konten, Spiegelkonten, Garantiekonten). Ein Nebensystem, das die ASI-Schnittstelle nutzt, kann bei Erfüllung der Teilnahmevoraussetzungen parallel dazu ein PM-Kontoinhaber werden und ein PM-Konto eröffnen.

[20] Weitere Einzelheiten finden sich im UDFS-Buch 1, Kapitel 2.8 („Settlement of ancillary systems“).

Es könnte somit die ASI für seine Abwicklungsaktivitäten und das PM-Konto für andere Zwecke verwenden. Um unterschiedliche Geschäftsfälle im Zusammenhang mit den verschiedenen Nebensystemen zu unterstützen, bietet das Zahlungsmodul über die ASI sechs generische Abwicklungsverfahren.

Abwicklungsverfahren[21]	Beschreibung
Verfahren 1 Liquiditätsübertragung	Liquidtätsübertragung zwischen einem Nebensystem-Teilnehmer und dem PM über ein Spiegelkonto. Die Verrechnung erfolgt im Nebensystem selbst.
Verfahren 2 Abwicklung in Echtzeit	Übertragung zwischen den Konten zweier PM-Kontoinhaber mit dem Ziel, eine im Nebensystem bereits ausgleichsfähige Transaktion endgültig abzuschließen.
Verfahren 3 Bilaterale Abwicklung	Das Nebensystem übermittelt dem PM Belastungen und Gutschriften gleichzeitig. Die beiden Transaktionen („credit leg“ und „debit leg“) werden unabhängig voneinander abgewickelt.
Verfahren 4 Multilaterale Standardabwicklung	Belastungen und Gutschriften werden gleichzeitig an das PM übermittelt. Erst wenn alle Belastungen erfolgreich verarbeitet wurden, werden die Gutschriften verbucht.
Verfahren 5 Simultan-multilaterale Abwicklung	Belastungen und Gutschriften werden gleichzeitig an das PM übermittelt. Sie werden jedoch sämtlich auf ihre Abwicklungsfähigkeit geprüft und können nur nach dem Grundsatz „alles oder nichts“ abgewickelt werden.
Verfahren 6 Dedizierte Liquidität und systemübergreifende Abwicklung	PM-Kontoinhaber dedizieren Liquidität zur Abwicklung der Nebensystem-Transaktionen entweder auf speziellen Unterkonten oder auf dem Spiegelkonto („Mirror Account“). Die Abwicklung erfolgt entweder auf den Unterkonten oder im Nebensystem selbst. Dieses Abwicklungsverfahren eignet sich besonders für das Nachtgeschäft, kann jedoch auch während des Tages verwendet werden.

Tabelle 5: Abwicklungsverfahren

Außerdem können die oben erwähnten obligatorischen Abwicklungsverfahren durch nachstehend aufgeführte Mechanismen den besonderen Bedürfnissen der einzelnen Nebensysteme angepasst werden:

- Informationsfrist zur Vorankündigung einer Abwicklung nach den AS-Verfahren 3, 4 und 5;

[21] Integriertes Modell: Die endgültige geldliche Verrechnung findet im Wertpapierabwicklungssystem selbst statt._Schnittstellen-Modell: Die endgültige geldliche Verrechnung findet im Zahlungsmodul statt.

- Abwicklungszeitraum für den Saldenausgleich der Nebensysteme, um die Abwicklung anderer Geschäfte nicht zu behindern; sind die Nebensystem-Transaktionen am Ende dieses Zeitraums nicht abgewickelt, werden die entsprechenden Salden entweder zurückgewiesen oder es wird ein Garantiekonto-Verfahren aktiviert, sofern dies vom Nebensystem für die Verfahren 4 und 5 festgelegt wurde.
- Durch ein Garantiekonto-Verfahren wird die erforderliche zusätzliche Liquidität bereitgestellt, wenn Nebensystem-Transaktionen mit der vorhandenen Liquidität der Teilnehmer nicht abgewickelt werden können.
- Der festgelegte Zeitpunkt („scheduled time“) ist ein Mechanismus, der Nebensystem-Transaktionen bis zum festgelegten Abwicklungszeitpunkt speichert.

Nebensysteme, die die Abwicklungsverfahren 3, 4, 5 und 6 einsetzen, können SWIFTNet FileAct nutzen, um die Geldseite von AS-Transaktionen abzuwickeln. Für Abwicklungsverfahren 6 genutzte SWIFTNet FileAct-Nachrichten können grundsätzlich über die gesamte Öffnungszeit des Zahlungsmoduls hinweg verarbeitet werden, d. h. bis zum Annahmeschluss für Interbankzahlungen (18.00 Uhr) und ab dem Beginn der Nachtverarbeitung (19.30 Uhr), ausgenommen die für Wartungsarbeiten an der Gemeinschaftsplattform vorgesehenen Zeitfenster. Für Abwicklungsverfahren 3, 4, und 5 genutzte SWIFTNet FileAct-Nachrichten können während der Tagverarbeitung von 7.00 Uhr bis 18.00 Uhr verarbeitet werden.

3 Teilnahme

3.1 Zugangskriterien

Das Eurosystem hat die allgemeine rechtliche Struktur und die Grundsätze für die Teilnahme an TARGET2 so gestaltet, dass die TARGET2-Nutzer entscheiden können, in welcher Form sie am System teilnehmen. Der Zugang zum TARGET2-System kann auf verschiedene Weise erfolgen: über die direkte oder eine indirekte Teilnahme, über „erreichbare BIC-Inhaber“[22] oder über den „Multi-Adressaten-Zugang“. Die TARGET2-Nutzer müssen die in Abschnitt 3.5 beschriebenen TARGET2-Sicherheitsanforderungen und -kontrollen erfüllen.

3.1.1 Direkte Teilnahme

Zugelassen für die direkte Teilnahme an TARGET2 sind:

a) Kreditinstitute, die ihren Sitz oder eine ihrer Zweigstellen im Europäischen Wirtschaftsraum (EWR) haben, auch wenn sie über eine im EWR ansässige Zweigstelle handeln

b) Kreditinstitute mit Sitz außerhalb des EWR, sofern sie über eine im EWR ansässige Zweigstelle handeln

c) NZBen der EU-Mitgliedstaaten und die EZB.

Die zuständige Zentralbank kann nach ihrem Ermessen darüber hinaus als direkte Teilnehmer zulassen:

a) am Geldmarkt aktive (Haupt-)Kassen/(zentrale) Finanzabteilungen von Zentral- oder Regionalregierungen der EU-Mitgliedstaaten

b) öffentliche Stellen von EU-Mitgliedstaaten, die zur Führung von Kundenkonten berechtigt sind

c) Wertpapierfirmen mit Sitz oder Zweigstelle im EWR

d) Stellen, die Nebensysteme betreiben und in dieser Funktion handeln

e) Kreditinstitute oder Stellen der unter a) bis d) aufgeführten Art, sofern diese ihren Sitz in einem Land haben, mit dem die Europäische Union eine Währungsvereinbarung getroffen hat, wonach solchen Stellen der Zugang zu Zahlungsverkehrssystemen in der Europäischen Union gestattet ist. Dies gilt nur nach Maßgabe der in der Währungsvereinbarung festgelegten Bedingungen und

[22] Der BIC (Business Identifier Code) ist die international am häufigsten verwendete Art der Identifizierung von Finanzinstituten. In seiner Funktion als ISO-Registrierungsstelle gibt SWIFT an Finanzinstitute und Nicht-Finanzinstitute, die an SWIFT angeschlossen sind, sowie an nicht angeschlossene Institute BICs aus. Der BIC wird für Finanztransaktionen, Datenbanken im Zusammenhang mit Kunden- und Geschäftspartnern, Compliance-Dokumente und sonstige Zwecke genutzt. Die BIC-Struktur basiert auf ISO 9362 (siehe SWIFT-Website).

unter der Voraussetzung, dass die in dem betreffenden Land geltenden rechtlichen Regelungen den einschlägigen Rechtsvorschriften der Europäischen Union entsprechen.

Direkte Teilnehmer sind Stellen, die mindestens ein PM-Konto im Zahlungsmodul (Payment Module – PM) der Gemeinschaftsplattform (Single Shared Platform – SSP) unterhalten (PM-Kontoinhaber) und/oder über ein Geldkonto auf der T2S-Plattform verfügen (Geldkontoinhaber). Die PM-Kontoinhaber erhalten über SWIFT oder Internet Zugang zur Gemeinschaftsplattform (jeweils PM-Kontoinhaber mit SWIFT-basiertem Zugang oder PM-Kontoinhaber mit internetbasiertem Zugang). Für den internetbasierten Zugang gelten Sonderregeln, die in Abschnitt „3.2 Internetbasierter Zugang“ erläutert werden.

Der Zugriff des Geldkontoinhabers oder des in dessen Namen handelnden Inhabers des PM-Hauptkontos auf das Geldkonto erfolgt über *a)* eine direkte Verbindung zur T2S-Plattform durch einen für T2S lizenzierten Anbieter von Mehrwertnetzwerkdiensten (value-added network service provider – VA-NSP) (direkt angeschlossene Geldkontoinhaber) und/oder *b)* eine indirekte Verbindung über die TARGET2-Zusatzleistungen (value-added services – VAS) für T2S (indirekt angeschlossene Geldkontoinhaber).

Direkte Teilnehmer können*:*

a) Zahlungen direkt in die/aus der Gemeinschafts-/T2S-Plattform einreichen/empfangen;

b) Zahlungen direkt über ihre Zentralbank abwickeln;

c) PM-Sonderkonten für nicht mit dem Zahlungsverkehr zusammenhängende Aktivitäten eröffnen (z. B. für die Erfüllung der Mindestreservepflicht). Diese Sonderkonten werden anhand eines separaten BIC11 identifiziert.

Darüber hinaus sind die PM-Kontoinhaber verantwortlich für alle über ihr Konto eingereichten Zahlungen an Stellen bzw. auf ihrem Konto empfangenen Zahlungen der Stellen, die über sie in TARGET2 registriert sind (indirekte Teilnehmer, Stellen mit Multi-Adressaten-Zugang und erreichbare BIC-Inhaber (siehe unten)).

Gemäß den TARGET2-Bedingungen der jeweiligen Zentralbank wird davon ausgegangen, dass die Teilnehmer Kenntnis von allen für sie geltenden Verpflichtungen aus Rechtsvorschriften zum Datenschutz sowie zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung, proliferationsrelevanter nuklearer Tätigkeiten und der Entwicklung von Trägersystemen für Kernwaffen besitzen und diese erfüllen. Weitere Informationen zu diesen Verpflichtungen können die Teilnehmer den von der jeweiligen Zentralbank veröffentlichten Bedingungen entnehmen.

3.1.2 Indirekte Teilnahme

Kreditinstitute mit Sitz im EWR können jeweils mit (nur) einem PM-Kontoinhaber vertraglich vereinbaren, Zahlungsaufträge einzureichen und/oder Zahlungen zu empfangen, die über das PM-Konto dieses PM-Kontoinhabers verrechnet werden. Zentralbanken erkennen indirekte Teilnehmer durch deren Aufnahme in das TARGET2-Directory an.

Sofern ein PM-Kontoinhaber, bei dem es sich um ein Kreditinstitut handelt, und ein indirekter Teilnehmer derselben Gruppe angehören, kann der PM-Kontoinhaber dem indirekten Teilnehmer ausdrücklich gestatten, das PM-Konto unmittelbar zu nutzen, um im Wege des gruppenbezogenen Multi-Adressaten-Zugangs Zahlungsaufträge einzureichen und Zahlungen zu empfangen.

3.1.3 Multi-Adressaten-Zugang

PM-Kontoinhaber können ihre Zweigstellen oder ihrer Gruppe angehörende Kreditinstitute, die sich in EWR-Ländern befinden, bevollmächtigen, ohne die Mitwirkung des PM-Kontoinhabers Zahlungen über ihr Konto abzuwickeln, indem die Zahlungen direkt in die Gemeinschaftsplattform eingereicht bzw. über diese empfangen werden. Dies bietet den Niederlassungen von Banken oder Bankengruppen effiziente Mechanismen für das Liquiditätsmanagement und Zahlungsverkehrsgeschäft.

Der Multi-Adressaten-Zugang kann wie folgt gewährt werden:

a) Ein Kreditinstitut, das als PM-Kontoinhaber zugelassen wurde, kann einer oder mehreren seiner im EWR ansässigen Zweigstellen zur direkten Einreichung von Zahlungsaufträgen und/oder zum direkten Empfang von Zahlungen Zugang zu seinem PM-Konto gewähren, sofern die betreffende Zentralbank darüber informiert wurde.

b) Wurde eine Zweigstelle eines Kreditinstituts als PM-Kontoinhaber zugelassen, so haben auch die anderen Zweigstellen derselben juristischen Person und/oder die Zentrale - vorausgesetzt, sie sind im EWR ansässig - Zugang zum PM-Konto jener Zweigstelle, sofern die betreffende Zentralbank darüber informiert wurde.

In der Praxis kann eine Bank mit Multi-Adressaten-Zugang ihren Zahlungsverkehr über ihre eigene BIC-Adresse abwickeln. Die Zahlungen werden jedoch auf dem Konto ihres PM-Kontoinhabers verbucht.

3.1.4 Erreichbare BIC-Inhaber

Die erreichbaren BIC-Inhaber in TARGET2 unterliegen keinerlei Systemregelungen. Alle Korrespondenten und Zweigstellen eines PM-Kontoinhabers, die Inhaber eines BIC sind, können unabhängig von ihrem Sitz in das TARGET2-Directory aufgenommen werden. Darüber hinaus wurden vom Eurosystem für diese erreichbaren BIC-Inhaber keine finanziellen oder administrativen Kriterien ausgearbeitet, sodass die Festlegung einer Vermarktungsstrategie für diesen Status dem PM-Kontoinhaber obliegt. Der PM-Kontoinhaber ist dafür verantwortlich, die für die Aufnahme in das TARGET2- Directory relevanten Informationen an die betreffende Zentralbank weiterzuleiten.

Zahlungsaufträge von/an erreichbare(n) BIC-Inhaber(n) werden immer über einen PM-Kontoinhaber eingereicht bzw. empfangen. Ihre Zahlungen werden über das Konto des PM-Kontoinhabers im Zahlungsmodul der Gemeinschaftsplattform abgewickelt.

		Konto	Einreichung/ Empfang von Zahlungen	Zahlungs-abwicklung	Unterliegt System-regelungen	Aufgeführt im TARGET2-Directory
Direkte Teilnahme	**PM-Kontoinhaber**	PM-Konto	Direkt	Eigenes Konto im PM	Ja	Ja
	Geldkonto-inhaber	Geld-konto	Direkt	Eigenes Konto auf der T2S-Plattform	Ja	Nein
Multi-Adressaten- Zugang		Kein Konto	Direkt	Konto des direkten Teilnehmers	Ja	Ja
Indirekte Teilnahme		Kein Konto	Über den direkten Teilnehmer	Konto des direkten Teilnehmers	Ja	Ja
Erreichbare BIC-Inhaber		Kein Konto	Über den direkten Teilnehmer	Konto des direkten Teilnehmers	Nein	Ja

Tabelle 6: TARGET2-Teilnahmestruktur

3.1.5 Kontengruppe

Den Status „Kontengruppe“ können verschiedene Kategorien von Instituten erlangen:

Kategorie 1: Kreditinstitute, die gemäß den International Accounting Standards (IAS 27) konsolidieren,

Kategorie 2: Kreditinstitute, die nicht oder gemäß anderen Standards konsolidieren, welche jedoch der im IAS 27 enthaltenen Definition entsprechen,

Kategorie 3: bilaterale und multilaterale Netzwerke von Sparkassen und Genossenschaftsbanken, für die satzungsmäßige Regelungen/Kooperationsregelungen gelten, die die nationalen rechtlichen Anforderungen erfüllen.

Dementsprechend wird bei einem Antrag auf Anerkennung des Gruppenstatus folgendermaßen verfahren:

Kategorie 1: Einreichung eines Auszugs aus dem offiziellen konsolidierten Jahresabschluss oder einer beglaubigten Erklärung eines externen Rechnungsprüfers, worin angegeben ist, welche Stellen in die Konsolidierung einbezogen sind.

Kategorie 2: Einreichung einer Erklärung eines externen Rechnungsprüfers, die gegenüber der NZB darlegt, dass die Konsolidierung dem IAS 27 entspricht.

Kategorie 3: Die NZB erstellt zunächst eine Beurteilung, in der dargelegt wird, dass die „Gruppe“ mit den nationalen rechtlichen Anforderungen und/oder dem rechtlichen Rahmen im Einklang steht, und dass sie die im TARGET2-Rechtsrahmen festgelegten politischen Vorgaben erfüllt. Darüber hinaus muss der EZB-Rat dem Antrag auf Anerkennung als Gruppe zustimmen.

3.2 Internetbasierter Zugang

Der internetbasierte Zugang zu TARGET2 stellt eine alternative Art der Verbindung mit der Gemeinschaftsplattform dar, die einen direkten Zugriff auf die wichtigsten TARGET2-Dienstleistungen bietet,[23] ohne dass eine Verbindung mit dem SWIFT-Netzwerk erforderlich ist. Dementsprechend senden und erhalten Teilnehmer mit internetbasiertem Zugang keine Nachrichten über das SWIFT-Netzwerk, sondern verwenden das ICM, um Zahlungen über die SSP zu veranlassen und Informationen über eingehende Zahlungen sowie Kontoauszüge zu erhalten.

Der internetbasierte Zugang unterstützt folgende Funktionen:

- Überwachung eines PM-Kontos über das ICM, einschließlich der Bereitstellung von Online-Informationen über ein- und ausgehende Zahlungen (final oder schwebend) sowie über die Verrechnung von Nebensystemen und Liquiditätspositionen,

[23] Teilnehmer können über einen internetbasierten Zugang auf ein PM-Konto oder ein HAM-Konto zugreifen.

- Erstellung von Überweisungen über spezielle ICM-Erfassungsmasken, einschließlich MT 103/MT 103STP, MT 202/MT 202COV und Liquiditätsüberträgen an Teilnehmer mit SWIFT-basiertem oder internetbasiertem Zugang,
- Anzeige eingehender Überweisungen von Teilnehmern mit SWIFT-basiertem Zugang oder internetbasiertem Zugang, einschließlich MT 103/MT 103STP, MT 202/MT 202COV und Liquiditätsübertragungen, sowie MT 204 von Teilnehmern mit SWIFT-basiertem Zugang,
- Anzeige von Benachrichtigungen, Informationen und Tagesabschlussnachrichten über das ICM. Am Beginn des nächsten Geschäftstages kann ein Kontoauszug heruntergeladen werden.
- Verwaltung von Limiten und Reservierungen; Verwaltung von in der Warteschlange stehenden Aufträgen, einschließlich der Änderung von Prioritäten, der Umsortierung von Zahlungsaufträgen, der Änderung von Ausführungsfristen und der Stornierung von Zahlungen in der Warteschlange,
- Abwicklung der Position eines Teilnehmers innerhalb der Verrechnung eines Nebensystems, einschließlich AS-Abwicklungsverfahren 6, für das Unterkonten eröffnet werden können,
- Abwicklung von Zahlungen im Rahmen von Offenmarktgeschäften des Eurosystems,
- Online-Einsicht in das TARGET2-Directory.

Dabei ist Folgendes zu beachten:

- PM-Kontoinhaber mit internetbasiertem Zugang können nur im User-to-Application-Modus (U2A) auf das ICM zugreifen.
- Im Fall von Kontengruppen, Multi-Adressaten-Zugängen oder erreichbaren BIC-Inhabern ist die Verwendung eines internetbasierten PM-Kontos nicht möglich.
- Einem PM-Kontoinhaber mit internetbasiertem Zugang stehen die TARGET2-Zusatzleistungen für T2S nicht zur Verfügung.
- Ein PM-Kontoinhaber mit internetbasiertem Zugang kann nicht zum Inhaber des PM-Hauptkontos für ein Geldkonto bestimmt werden.
- Aus Sicherheitsgründen steht zwischen 22.00 Uhr und 6.30 Uhr keine Internetverbindung zur Verfügung. Darüber hinaus können von 19.30 Uhr bis 22.00 Uhr sowie zwischen 6.30 Uhr und 6.45 Uhr - mit Ausnahme von Liquiditätsübertragungen - keine Zahlungen getätigt werden.

3.3 Anbindung und Registrierung

3.3.1 Anbindung an die Gemeinschaftsplattform

Zur Einrichtung einer Verbindung zur SSP müssen sich PM-Kontoinhaber, die einen SWIFT-basierten Zugang haben möchten, bei SWIFT, und um einen internetbasierten Zugang zu erhalten, bei einer akkreditierten Zertifizierungsstelle registrieren.

Bei PM-Kontoinhabern mit internetbasiertem Zugang sollte die Registrierung bei einer akkreditierten Zertifizierungsstelle entsprechend den im „User manual internet access for the public key certification service (Benutzerhandbuch zur Public-Key-Zertifizierung für den Internetzugang)“ spezifizierten Verfahren durchgeführt werden. Das Benutzerhandbuch ist auf den TARGET2-Internetseiten der Bundesbank verfügbar.

Durch die Registrierung bei SWIFT können PM-Kontoinhaber mit SWIFT-basiertem Zugang die geeigneten SWIFT-Dienste für TARGET2 in Anspruch nehmen. Die Registrierung geschieht über ein von SWIFT entwickeltes, auf TARGET2 zugeschnittenes elektronisches Formular auf der SWIFT-Website (sog. „E-Ordering“), wobei die Aktualisierung der Angaben im BIC-Directory nur einmal pro Monat erfolgt. Im Rahmen des E-Ordering müssen alle Anmeldeanträge zunächst durch die Zentralbanken validiert und genehmigt werden und danach die Zustimmung durch den SSP Service Desk erhalten. Das gesamte Verfahren einschließlich Validierung und Umsetzung durch SWIFT kann zwei bis fünf Wochen in Anspruch nehmen. Zur Gewährleistung übereinstimmender Stammdaten bei SWIFT und auf der SSP sollten PM-Kontoinhaber bei Änderungen jeglicher Art – insbesondere im Bereich der Message Routing Rules (MRR) – vorzugsweise die E-Ordering-Funktion per www.swift.com nutzen. Verwendet der PM-Kontoinhaber hierzu „myswift.com“, also eine SWIFT Customer Relationship Management Website, sollte die Änderung mit der Zentralbank abgesprochen werden. Die Zentralbank ist vor dem Umsetzungsdatum zu informieren. Weitere Informationen zur Registrierung bei SWIFT stehen auf www.swift.com zur Verfügung.

Zusätzlich zur Registrierung bei SWIFT benötigen PM-Kontoinhaber mit SWIFT-basiertem Zugang eine RMA-Autorisierung mit TRGTXEPM, Inhaber von HAM-Konten eine mit TRGTXEHM, der Co-Manager von HAM-Konten eine mit TRGTXEPM und TRGTXEHM und Zentralbankkunden eine mit TRGTXECB. Dieser Schritt ist für alle PM- und HAM-Kontoinhaber sowie für Zentralbankkunden obligatorisch.

3.3.2 Anbindung an die T2S-Plattform

Zur Einrichtung einer direkten Verbindung zur T2S-Plattform müssen die Geldkontoinhaber (**direkt angeschlossene Geldkontoinhaber**) einen[24] für TS2 lizenzierten Anbieter von Mehrwertnetzwerkdiensten (value-added network service provider – VA-NSP) auswählen und die T2S-Verbindungsdienste über die VA-NSP-Website abonnieren. Der Antrag muss zunächst von der Zentralbank und danach vom T2S Service Desk geprüft und genehmigt werden. Der Geldkontoinhaber wird per E-Mail über jede sich in Bezug auf den Status des Antrags ergebende Änderung informiert. Bei Ablehnung des Antrags wird der jeweilige Grund genannt. Bei Annahme des Antrags erfolgt nach Festlegung des Umsetzungsdatums eine abschließende Bestätigung. Am Umsetzungsdatum stellt der Anbieter der Mehrwertnetzwerkdienste die Dienstleistungen in der beantragten Form bereit und übermittelt dem Geldkontoinhaber eine abschließende Bestätigung.

Dabei ist Folgendes zu beachten: Ist ein Geldkontoinhaber auch Kunde eines Zentralverwahrers oder einer anderen Zentralbank, so muss dieser Schritt nur einmal durchgeführt werden. Auf Anfrage kann der T2S Service Desk einer Zentralbank mitteilen, ob der Geldkontoinhaber bereits für die T2S-Verbindungsdienste registriert ist oder nicht.

Zusätzlich zu den T2S-Verbindungsdiensten sollte der Geldkontoinhaber beim Anbieter der Mehrwertnetzwerkdienste auch die Ausstellung digitaler Zertifikate für Authentifizierungs- und Signaturzwecke beantragen. Diese Zertifikate können auf USB-Token für den U2A-Zugriff durch Endnutzer oder auf dem Hardware-Sicherheitsmodul (HSM) für den A2A-Zugriff durch Anwendungen zur Verfügung gestellt werden.

Weitere Informationen finden sich in der VA-NSP-Dokumentation und in den folgenden Dokumenten: T2S Connectivity Licences and Licence Agreement und T2S Connectivity Guide.

Bei **indirekt angeschlossenen Geldkontoinhabern** ist keine Registrierung über einen Anbieter von Mehrwertnetzwerkdiensten erforderlich. Es reicht aus, wenn der Inhaber des PM-Hauptkontos die TARGET2-Mehrwertdienste für T2S anhand der SSP-Registrierungsformulare abonniert (siehe Abschnitt unten).

3.3.3 Erhebung von Stammdaten

Jeder Nutzer muss der Zentralbank seine Stammdaten zur Verfügung stellen. An die Gemeinschaftsplattform angebundene Nutzer verwenden hierzu die SSP-Formulare und

[24] Direkt angeschlossene Geldkontoinhaber können beide Netzdienstanbieter in Anspruch nehmen, z. B. aus Gründen der Business Continuity.

Geldkontoinhaber die DCA-Formulare. Die Formulare können die Nutzer auf dem mit ihrer Zentralbank vereinbarten Weg beim jeweiligen National Service Desk einreichen.

Die Zentralbanken geben die Formularangaben der an die Gemeinschaftsplattform angebundenen Nutzer über das ICM[25] und die der Geldkontoinhaber über die T2S GUI ein[26].

Aus verfahrenstechnischer Sicht sind vier Schritte einzuhalten:

- **Analyse**

Der Nutzer analysiert im Rahmen seines Change-Management-Verfahrens die nötigen Änderungen und füllt die entsprechenden Formulare aus, die anschließend der betreffenden Zentralbank übermittelt werden.

Änderungen an den Stammdaten nimmt der Nutzer überwiegend in eigener Regie vor. Er definiert seine Anforderungen, wobei er vielfach mit SWIFT und/oder dem Anbieter von Mehrwertnetzwerkdiensten und/oder der Zentralbank in Kontakt steht, um sich über die Durchführbarkeit zu informieren. Vor allem bei komplexen Änderungen ist eine vorherige Kommunikation mit der Zentralbank notwendig. Dabei sollten die Nutzer mit der Darstellung ihrer geplanten Änderung beginnen. Die Dauer der Analyse hängt von der Organisation des Nutzers ab.

Der Nutzer übermittelt seiner Zentralbank die Registrierungsformulare und gegebenenfalls:

- eine Darstellung der Änderung und des Verfahrens (z. B. Kontokonfiguration, technische Änderungen, Bedarf an spezifischen Tests und Support);
- eine einschlägige Rechtsdokumentation (z. B. Ländergutachten);
- eine technische Dokumentation (z. B. zur Ausfallsicherheit).

- **Bewertung und Validierung**

Im Falle umfangreicher Änderungen sollte die zuständige Zentralbank in die oben beschriebene Analyse einbezogen werden. Diese prüft die Formulare in rechtlicher und technischer Hinsicht nach Maßgabe ihrer nationalen Bestimmungen. Ferner kontrolliert die Zentralbank, ob die Registrierung bei SWIFT/beim Anbieter von Mehrwertnetzwerkdiensten mit den Angaben in den Stammdatenformularen übereinstimmt.

25 Weitere Informationen und ausführliche Erläuterungen zu den Formularen sind dem Dokument User guide for collection of static data zu entnehmen.

26 Ausführliche Erläuterungen zu den Formularen sind dem Dokument DCA registration Guide zu entnehmen.

Die Prüfungen durch die Zentralbank zielen auf die Gewährleistung der rechtlichen und operationellen Sicherheit des gesamten TARGET2-Systems ab.

Die Zentralbank muss überprüfen, ob die Nutzerzertifizierung unter den neuen Voraussetzungen noch gültig ist. Andernfalls muss eine neue Zertifizierungsphase (die inhaltlich vom gegenwärtigen Zertifizierungsstatus und der Art der anstehenden Änderung abhängt) geplant[27] und erfolgreich durchgeführt/zu einem erfolgreichen Abschluss gebracht werden. Ein Nutzer kann zudem beantragen, dass zunächst in der Testumgebung getestet wird, bevor der Live-Betrieb erfolgt. Die Prüfungen umfassen auch die Validierung der Registrierungsformulare.

Abschließend validiert die Zentralbank den Antrag oder lehnt ihn ab.

- **Durchführung der Stammdatenerhebung**

Nach der Validierung gibt die Zentralbank die Angaben aus den Formularen über das ICM und/oder die T2S GUI ein. Ergeben sich Auswirkungen für das TARGET2-Directory, ist die Frist für dessen wöchentliche Aktualisierung zu berücksichtigen.

- **Abschließende Prüfung**

Anhand des ICM oder der T2S GUI sollte der betreffende Nutzer die Richtigkeit des neuen Stammdateneintrags/der Änderung überprüfen.

3.3.3.1 Konfliktäre Registrierung von erreichbaren BIC-Inhabern und indirekten Teilnehmern

Das TARGET2-Directory erlaubt pro BIC[28] lediglich eine Anmeldung und nur eine Beziehung zwischen einem erreichbaren BIC-Inhaber/indirekten Teilnehmer und dem PM-Kontoinhaber, der den Zugang zu TARGET2 ermöglicht. Aus diesem Grund ist es möglich, dass zwei oder mehrere Teilnehmer konfliktäre Registrierungsformulare an ihre Zentralbank senden. Daher sollten die Banken, bevor sie ein Registrierungsformular an ihre Zentralbank schicken, um einen erreichbaren BIC-Inhaber zu registrieren, im TARGET2-Directory nachprüfen, ob der BIC, mit dem sie den erreichbaren BIC-Inhaber/indirekten Teilnehmer anmelden möchten, bereits bei einem anderen PM-Kontoinhaber registriert wurde.

Ist der erreichbare BIC-Inhaber/indirekte Teilnehmer (Bank X) schon im TARGET2-Directory bei einem anderen PM-Kontoinhaber B registriert, muss sich der antragstellende PM-Kontoinhaber A mit

[27] Je nach Änderung kann es sein, dass die geplante Modifizierung auch im Testumfeld vorgenommen werden muss.

[28] BIC mit elf Stellen.

dem anderen PM-Kontoinhaber B in Verbindung setzen, um diesen darüber zu informieren, dass sich die Routing-Anweisungen für den erreichbaren BIC-Inhaber/indirekten Teilnehmer (Bank X) ändern werden.

Der PM-Kontoinhaber B, über den gegenwärtig die Verbindung der Bank X besteht, muss dann ein Formular ausfüllen und die Löschung der bestehenden Registrierung beantragen. Dieses Formular reicht er bei seiner Zentralbank und dem PM-Kontoinhaber A ein.

Der PM-Kontoinhaber A leitet daraufhin sein eigenes Formular für die Registrierung des erreichbaren BIC-Inhabers/indirekten Teilnehmers (Bank X) mit einer Kopie des vom anderen PM-Kontoinhaber B unterzeichneten Formulars für die Aufhebung der früheren Verbindung an seine Zentralbank weiter.

Falls der erreichbare BIC-Inhaber/indirekte Teilnehmer zu dem Zeitpunkt, zu dem der PM-Kontoinhaber die Überprüfung durchführt, nicht im TARGET2-Directory aufgeführt ist, aber in der gleichen Woche ein anderer PM-Kontoinhaber die Anmeldung desselben BIC-Inhabers als erreichbaren BIC-Inhaber/indirekten Teilnehmer beantragt, wird einer der Zentralbankanträge abgelehnt. Die betreffende Zentralbank muss dann die Banken von den konfliktären Registrierungsaufträgen in Kenntnis setzen. Es obliegt den Banken, eine Vereinbarung zu erzielen, welche Bank der PM-Kontoinhaber sein soll, der den Korrespondenten vertritt.

3.3.3.2 TARGET2-Directory

Das TARGET2-Directory unterstützt das Routing von Zahlungsaufträgen. Es verwendet mit SWIFT zusammenhängende Informationen in Verbindung mit TARGET2-spezifischen Informationen, die die PM-Kontoinhaber im Rahmen der SSP-Registrierung bereitstellen. Das TARGET2-Directory ist die Datenbank, der die BICs für das Routing von Zahlungsaufträgen entnommen werden können.

Sofern vom TARGET2-Nutzer nicht anders gewünscht, werden die BICs im TARGET2-Directory veröffentlicht.[29]

Der Inhalt des TARGET2-Directory basiert auf den Stammdaten der Gemeinschaftsplattform, wie sie bei den PM-Kontoinhabern mittels dafür vorgesehener Formulare erhoben wurden. Diese Formulare werden von den PM-Kontoinhabern verwendet, um die Eröffnung ihres Kontos/ihrer Konten zu beantragen und alle anderen vom System benötigten Informationen einzuholen. Der PM-Kontoinhaber ist insbesondere für die Anmeldung seiner indirekten Teilnehmer, Stellen mit Multi-Adressaten-Zugang oder erreichbaren BIC-Inhaber verantwortlich und für alle dabei auftretenden Fehler oder missbräuchlichen Verwendungen haftbar.

[29] Die nicht im TARGET2-Directory veröffentlichten BICs werden jedoch im BIC-Directory von SWIFT publiziert.

Das TARGET2-Directory enthält Informationen zu allen Kreditinstituten, die über TARGET2 erreicht werden können. Es enthält außer dem BIC des Teilnehmers auch den BIC des Empfängers (d. h. den BIC, der zum Empfang und zum Versand von Zahlungen verwendet wird), des Kontoinhabers (d. h. den BIC des PM-Kontos), den Namen des Instituts, die Anschrift sowie die nationale Bankleitzahl (sofern vorhanden). Die folgende Tabelle ist ein Beispiel für einen Eintrag eines PM-Kontoinhaber im TARGET2-Directory:

Feld im TARGET2-Directory	Beispiel
BIC	BANKBEBBXXX
Addressee	BANKBEBBXXX
Account holder	BANKBEBBXXX
Institution name	Bank S.A. Brussels
City heading	Brussels
National sorting code	–
Main BIC flag	Yes
Type of change	A
Valid from	20080218
Valid until	99991231
Type of participation	01

Tabelle 7: TARGET2-Directory

Das TARGET2-Directory wird nur an PM-Kontoinhaber ausgegeben.[30] Die Verteilung erfolgt über SWIFTNet FileAct (für das gesamte Directory nur im „Pull"-Modus, für Aktualisierungen im „Pull"- und „Push"-Modus). Das Herunterladen des gesamten Inhalts ist in erster Linie für das erste Laden des Directory oder für den Fall vorgesehen, dass eine Wiederherstellung des Directory erforderlich ist. Aufgrund der Dateigröße wird eine Komprimierung nachdrücklich empfohlen. Des Weiteren können PM-Kontoinhaber das TARGET2-Directory zentral herunterladen und es intern verteilen. Sie dürfen das TARGET2-Directory nur an ihre Zweigstellen und Stellen mit Multi-Adressaten-Zugang weitergeben. Die Weitergabe an sonstige Dritte auf anderem Wege ist ihnen nicht gestattet.

Das TARGET2-Directory erscheint nicht in Papierform. Es wird wöchentlich aktualisiert. Die Aktualisierungen werden in der Nacht von Donnerstag auf Freitag bereitgestellt und gelten ab dem

[30] Teilnehmer mit internetbasiertem Zugang können das TARGET2-Directory online einsehen.

darauffolgenden Montag. Die vollständige Version steht ab Freitagmorgen zur Verfügung. PM-Kontoinhabern wird dringend empfohlen, ihren Zentralbanken Änderungsanträge frühzeitig zukommen zu lassen und dabei möglichst ein künftiges Aktivierungsdatum zu nennen. Für Änderungen der Stammdaten, die das TARGET2-Directory betreffen, ist es ratsam, einen Montag als Aktivierungsdatum zu wählen, um die Übereinstimmung der Stammdaten mit dem TARGET2-Directory sicherzustellen. Aus Gründen der Konsistenz ist es außerdem ratsam, den ersten Montag nach der monatlichen Aktualisierung des SWIFT BICPlusIBAN-Directory zu wählen.

3.3.3.3 Auf der T2S-Plattform aufgeführte externe RTGS-Konten

Auf der T2S-Plattform wird eine Liste externer RTGS-Konten geführt, anhand derer das Konto des Begünstigten bei ausgehenden Liquiditätsübertragungen (von einem Geldkonto auf ein PM-Konto) überprüft wird. Ist ein als Konto des Begünstigten angegebenes PM-Konto nicht auf der Liste externer RTGS-Konten zu finden, wird die Liquiditätsübertragung zurückgewiesen. Hierbei ist zu beachten, dass die auf dieser Liste stehenden Kontonummern für die direkt an T2S angeschlossen Geldkontoinhaber sichtbar sind. Es wird jedoch weder der BIC noch der Name des Instituts angezeigt, das das Konto unterhält, es sei denn, diese können von der PM-Kontonummer abgeleitet werden[31].

Dabei sind alle TARGET2-PM-Konten, die gegebenenfalls Liquiditätsübertragungen von einem Geldkonto empfangen können, in die T2S-Liste externer RTGS-Konten aufzunehmen, d. h. es werden alle Konten aufgeführt, mit Ausnahme von Spiegel-/technischen Konten, PM-Konten von Teilnehmern mit internetbasiertem Zugang sowie von unveröffentlichten Konten (unveröffentlichten BICs)[32].

Jede Zentralbank ist dafür verantwortlich, die T2S-Liste externer RTGS-Konten zu aktualisieren, wenn ein PM-Konto auf der Gemeinschaftsplattform eingerichtet, geändert oder gelöscht wird (mit Ausnahme eines Spiegel-/technischen Kontos, eines PM-Kontos eines Teilnehmers mit internetbasiertem Zugang sowie eines unveröffentlichten Kontos).

3.3.3.4 Informationsfluss zwischen Zentralbanken, DCA-Inhabern und Zentralverwahrern

Die Einrichtung und Schließung eines Geldkontos erfolgt durch die verantwortliche Zentralbank auf Basis der vom Geldkontoinhaber vorgelegten Stammdatenformulare. Nach Eröffnung des Geldkontos kann der Geldkontoinhaber seine(n) Zentralverwahrer kontaktieren, um die Kontokonfiguration

31 Jeder Geldkontoinhaber kann nur die Daten zu den PM-Konten einsehen, über die seine jeweilige Zentralbank verfügt.

32 Unveröffentlichte PM-Konten und PM-Konten von Teilnehmern mit internetbasiertem Zugang können von der Zentralbank auf Antrag des Teilnehmers in die Liste aufgenommen werden.

abzuschließen und die Verbindung vom Geldkonto zum Wertpapierkonto/zu den Wertpapierkonten herzustellen.

Beabsichtigt ein Geldkontoinhaber, ein Geldkonto zu schließen, hat er seine Zentralbank und seine(n) Zentralverwahrer hiervon in Kenntnis zu setzen. Anschließend hat er seine(n) Zentralverwahrer aufzufordern, die Verbindung(en) zwischen dem Geldkonto und dem Wertpapierkonto/den Wertpapierkonten aufzuheben. Nachdem alle Verbindungen gelöscht wurden, kann er die Schließung des Geldkontos bei der Zentralbank beantragen. Nach der Schließung ist es nicht mehr möglich, das Geldkonto für die Wertpapierabwicklung oder Liquiditätsübertragungen zu verwenden.

Es ist keine formelle Kommunikation zwischen den Zentralbanken und den Zentralverwahrern im Zusammenhang mit der Registrierung von Geldkontoinhabern vorgesehen. Bei der Eröffnung oder Schließung eines Geldkontos ist der Geldkontoinhaber dafür verantwortlich, die Einrichtung oder Aufhebung der Verbindung(en) zwischen dem Geldkonto und dem Wertpapierkonto/den Wertpapierkonten beim jeweiligen Zentralverwahrer/bei den jeweiligen Zentralverwahrern zu beantragen.

Tritt eine Sondersituation ein, wie beispielsweise die Insolvenz eines Geldkontoinhabers, die eine Zentralbank gegebenenfalls zur Sperrung des Geldkontos veranlasst, informiert die Zentralbank den/die Zentralverwahrer mittels einer GUI-Nachricht.

3.3.3.5 Verwaltung der Zugriffsrechte von direkt angeschlossenen DCA-Inhabern

Die Verwaltung der Zugriffsrechte in T2S ist dezentral organisiert und folgt dem dreistufigen Hierarchie-Modell der T2S-Parteien (siehe nachstehende Abbildung). Gemäß diesem Modell ist der Betreiber von T2S (4ZB) die auf der obersten Hierarchieebene angesiedelte Party. Zentralbanken und Zentralverwahrer befinden sich auf der zweiten Ebene, während ihre Teilnehmer (jeweils Geldkontoinhaber und CSD-Teilnehmer) die dritte Ebene bilden.

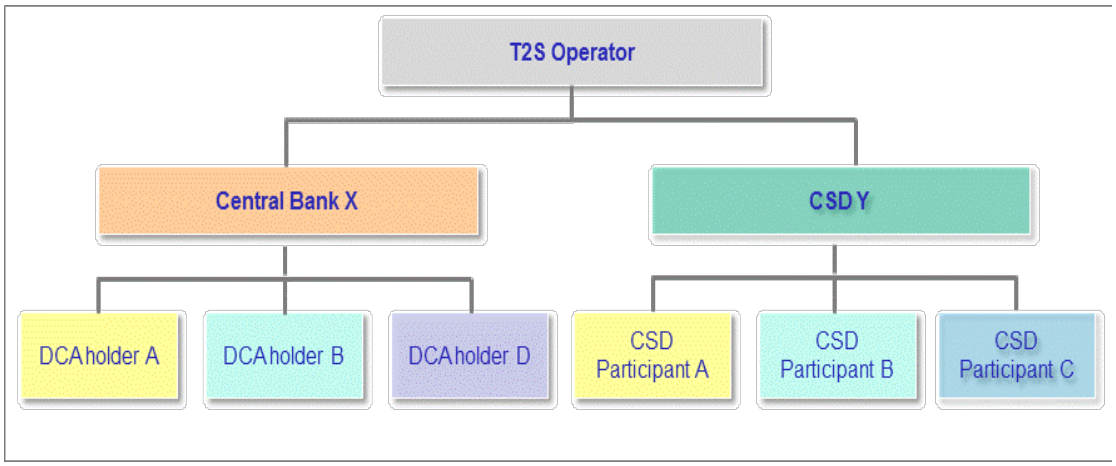


Abbildung 11: Hierarchie-Modell der T2S-Parties

Auf dieser Grundlage definiert der Betreiber von T2S über die Verwaltung der Zugriffsrechte die verschiedenen T2S-Funktionen, die von den Zentralbanken und Zentralverwahrern verwendet werden können. Die Zentralbanken und Zentralverwahrer wiederum definieren die verschiedenen T2S-Funktionen, die ihre Teilnehmer verwenden können. Der Umfang der Daten (Stamm- und transaktionsbezogene Daten), über die jede Einrichtung/Party verfügt, wird durch das Hierarchie-Modell der T2S-Parties bestimmt.

Ferner basiert die Verwaltung der Zugriffsrechte auf dem Konzept von Berechtigungen (privileges), Rollen (roles) und Party-Administratoren (party administrators). Unter Berechtigung ist das Recht zu verstehen, eine gewisse T2S-Funktion auszulösen (z. B. eine vorgegebene Abfrage auszuführen). Berechtigungen können in Rollen zusammengefasst werden. Das Zugangsrechteprofil eines bestimmten Nutzers ergibt sich aus den ihm übertragenen Rollen und Berechtigungen.

Jede Einrichtung/Party muss über mindestens einen Party-Administrator verfügen, d. h. einen Nutzer, der Rollen und Berechtigungen zuteilen darf, sofern sie der Einrichtung übertragen wurden, der er angehört. Der Party-Administrator kann über eine Berechtigung verfügen, sobald sie eingeräumt wurde. Ab diesem Zeitpunkt kann er die Berechtigung weitergeben. Nachdem die Zugangsrechte für eine Party auf der Ebene dieser Party konfiguriert wurden, kann der Party-Adminstrator/können die Party-Administratoren die Konfiguration diese Rechte auf Nutzerebene vornehmen, um allen Nutzern der Party die geeigneten Rollen und Berechtigungen zuzuweisen[33].

Rollen und Berechtigungen werden von den Party-Administratoren der einzelnen Stellen dezentral wie folgt gemäß dem Hierarchie-Modell der T2S-Parties vergeben:

(i) Der Administrator einer Zentralbank: a) erstellt neue Rollen, einschließlich der verfügbaren Berechtigungen; b) verwaltet die verfügbaren Rollen und Berechtigungen und weist sie den Nutzern zu; c) legt die ersten Administratoren seiner Geldkontoinhaber an; e) ordnet die verfügbaren Rollen und Berechtigungen seinen Geldkontoinhabern zu;

(ii) Der Administrator eines DCA-Inhabers: a) verwaltet die Nutzer seines Instituts; b) weist den Nutzern die verfügbaren Rollen und Berechtigungen zu.

[33] Wie im Dokument „Registration Guide for DCA Holders“ (Registrierungsanweisungen für DCA-Inhaber) angegeben, können die von den Zentralbanken bestimmten Administratoren für die Geldkontoinhaber dem Zwei-Augen- oder dem Vier-Augen-Prinzip unterworfen werden. Im Falle des Vier-Augen-Prinzips ist ein spezielles Verfahren anzuwenden. Um nähere Informationen zu erhalten, sollten die DCA-Inhaber ihre jeweilige Zentralbank kontaktieren.

Anmerkung:

- Der Anmeldename und die Unique System User Reference (spezifische Referenznummer des Systemnutzers) sollten gemäß der folgenden Struktur festgelegt werden: C (um anzuzeigen, dass es sich um einen Payment-Bank-Nutzer handelt) + Ländercode der Zentralbank (2 Zeichen) + BIC11 der Party + freier Text, der vom Geldkontoinhaber festgelegt wird und eine Länge von bis zu 21 Zeichen aufweisen kann.
- Die den Geldkontoinhabern zuzuweisenden Berechtigungen und Rollen werden in dem auf der TARGET2-Website abrufbaren Dokument „Registration Guide for DCA Holders“ erläutert.

3.4 Zertifizierungstests

Jeder TARGET2-Nutzer muss, abhängig von den von der betreffenden Zentralbank gewählten SSP-Modulen und den vom Nutzer gewählten Funktionen der Gemeinschafts- und/oder der T2S-Plattform, eine Reihe von Zertifizierungstests durchführen. Ein weiterer Faktor, der sich auf Art und Anzahl der durchzuführenden Tests auswirkt, ist beispielsweise die Teilnahme an verschiedenen Nebensystemen.

Die Zertifizierung lässt sich unterteilen in die technische Zertifizierung und die Feststellung der Betriebsbereitschaft:

- Die technische Zertifizierung der PM-Kontoinhaber und der Nebensysteme besteht aus dem erfolgreichen Abschluss einer gewissen Anzahl an Connectivity- und Interoperability-Tests. Die Feststellung der Betriebsbereitschaft wird auf Basis der Teilnahme an Country- und Business-Day-Tests geprüft.
- Die technische Zertifizierung der direkt angeschlossenen Geldkontoinhaber besteht aus dem erfolgreichen Abschluss einer gewissen Anzahl an Connectivity-, Certification- und Authorisation-Tests. Die Feststellung der Betriebsbereitschaft wird auf Basis der Teilnahme an Community- und Business-Day-Tests geprüft.
- Die technische Zertifizierung der indirekt angeschlossenen Geldkontoinhaber besteht aus dem erfolgreichen Abschluss einer gewissen Anzahl an Interoperability-, und Authorisation-Tests. Die Feststellung der Betriebsbereitschaft wird auf Basis der Teilnahme an Community- und Business-Day-Tests geprüft.

Weitere Informationen über die von den PM-Kontoinhabern, Nebensystemen und Geldkontoinhabern durchzuführenden Tests sind im „Guide to TARGET2 User Testing“ zu finden.

Das Testumfeld des Nutzers sollte der künftigen Produktivumgebung so weit wie möglich entsprechen. Jede verwendete Komponente sollte bereits ein internes Zulassungsverfahren durchlaufen haben.

Die zuständige Zentralbank muss schriftlich von allen während oder nach den Zertifizierungstests auftretenden Änderungen des Testumfelds und/oder der künftigen Produktivumgebung des Nutzers in Kenntnis gesetzt werden. Dazu gehören alle technischen Änderungen (z. B. an technischen Komponenten oder der Software) sowie sämtliche mit der Interaktion mit TARGET2 zusammenhängenden betrieblichen Änderungen. Unter einer betrieblichen Änderung ist eine Änderung der Kontenstruktur bzw. die Nutzung optionaler Funktionen zu verstehen, die in der Vergangenheit nicht genutzt wurden und deshalb nicht Teil eines früheren Zertifizierungsverfahrens waren. Die Mitteilung sollte neben einer eindeutigen Beschreibung von Art und Umfang der Änderung sowie der damit verbundenen Risiken einen Vorschlag enthalten, welche Testfälle aufgrund der Änderung erneut durchzuführen sind (Non-Regression-Tests). Die Zentralbank prüft diesen Vorschlag. Grundsätzlich sind während der technischen Zertifizierung Änderungen möglich; während der Feststellung der Betriebsbereitschaft sollten Änderungen vermieden werden. Änderungen nach der Zertifizierung eines TARGET2-Nutzers sind nicht mehr gestattet; sie würden ein neues Zertifizierungsverfahren erforderlich machen. Zur Wahrung der notwendigen Flexibilität können die Zentralbanken allerdings Ausnahmen von diesen Grundsätzen zulassen, sofern diese gerechtfertigt sind.

Der technische Aufbau der SSP und/oder der T2S-Plattform und/oder des PHA kann sich im Zuge der jährlichen Releases, nach Notfalländerungen und „Hot Fixes“ (z. B. zur Fehlerbehebung) ändern. In solchen Fällen schätzen die Zentralbanken ab, welche Auswirkungen diese Veränderungen auf das bereits von den TARGET2-Nutzern durchgeführte Zertifizierungsverfahren haben werden und informieren diese entsprechend. Unter Umständen kann es erforderlich sein, dass einige Zertifizierungstests wiederholt werden müssen (Non-Regression-Tests). Solche Aufforderungen zur Durchführung von Non-Regression-Tests werden auf das absolute Minimum begrenzt.

3.5 Maßnahmen zur Gewährleistung der Sicherheit und operationellen Zuverlässigkeit von TARGET2-Nutzern

3.5.1 Aufgaben und Zuständigkeiten

Folgende vier Hauptaufgaben und -zuständigkeiten sollen die Sicherheit und die operationelle Zuverlässigkeit der Nutzer gewährleisten:

- Festlegung des Rahmenwerks durch das Eurosystem: Verfassen von Richtlinien, an die sich alle beteiligten Parteien halten müssen, und Spezifizierung einheitlicher Anforderungen, die die Nutzer zu erfüllen haben
- Überprüfung auf Einhaltung durch die Zentralbanken („Compliance Check"): Überprüfung, ob die Nutzer die im Rahmenwerk festgelegten Maßnahmen einhalten
- Bereitstellung von Informationen durch Nutzer: Versorgung der Zentralbanken mit relevanten Informationen wie im Rahmenwerk festgelegt
- Überwachung und Folgemaßnahmen durch die Zentralbanken: Aufdeckung von Schwachstellen und Überwachung der Folgemaßnahmen, die diese Schwachstellen beseitigen sollen

Um sicherzustellen, dass alle Nutzer dieselben Kriterien erfüllen müssen und um eine harmonisierte Durchführung der „Compliance Checks" zu erleichtern, sind einheitliche und effektive Richtlinien sowie Verfahren erforderlich. Für die Festlegung und Einhaltung dieses Rahmenwerks ist das Eurosystem zuständig.

Was die „Compliance Checks" anbelangt, so gilt der Grundsatz, dass die Kundenbeziehung vollständig in den Zuständigkeitsbereich der Zentralbank fällt, die mit dem Nutzer in einer Rechtsbeziehung steht. Hierbei spielt es keine Rolle, ob der Nutzer seinen Sitz innerhalb oder außerhalb des Euro-Währungsgebiets hat. Vielmehr ist zu berücksichtigen, ob sich eine Zentralbank im TARGET2-Gebiet befindet[34].

Beispiele: Dänemark hat den Euro nicht eingeführt, aber die dänische Zentralbank nimmt an TARGET2 teil. Folglich gehen direkte Teilnehmer, deren Hauptsitz sich in Dänemark befindet, in der Regel mit der dänischen Zentralbank eine Rechtsbeziehung ein. Im Fall von direkten Teilnehmern mit Hauptsitz im Vereinigten Königreich ist dies anders. Die Bank of England hat sich entschieden, nicht an TARGET2 teilzunehmen. Deshalb müssen direkte Teilnehmer aus dem Vereinigten Königreich eine an TARGET2 teilnehmende Zentralbank auswählen, mit der sie eine Rechtsbeziehung eingehen.

Anhand der folgenden Fragen können die Zentralbanken feststellen, ob sie für das Einholen der relevanten Informationen bei einem bestimmten Nutzer zuständig sind.

Unterhält der Nutzer eine eigene technische Infrastruktur für das Routing von Zahlungen nach TARGET2?

- Lautet die Antwort „Ja": Die Zentralbank dieses direkten Teilnehmers ist die zuständige Zentralbank.

[34] Das TARGET2-Gebiet umfasst die Länder aller an TARGET2 teilnehmenden Zentralbanken.

- Lautet die Antwort „Nein“: Befindet sich die für das Routing von Zahlungen nach TARGET2 verwendete Infrastruktur, die von einem anderen direkten Teilnehmer unterhalten wird, in einem anderen Land (z. B. Mitglied/Konzentrator, Zweigstelle/Tochter, Zentrale eines direkten Teilnehmers)?
    - Lautet die Antwort „Ja“: Die Zentralbank des direkten Teilnehmers, der die technische Infrastruktur unterhält, ist zuständig.
    - Lautet die Antwort „Nein“: Bietet das Institut, das die Infrastruktur unterhält, den gleichen Service auch anderen direkten Teilnehmern an (z. B. Servicebüro)?
        - Lautet die Antwort „Ja“: Die Zentralbank, die mit dem betragsmäßig größten, diese Infrastruktur verwendenden direkten Teilnehmer in einer Rechtsbeziehung steht, ist zuständig.
        - Lautet die Antwort „Nein“: Die Zentralbank, die mit dem direkten Teilnehmer in einer Rechtsbeziehung steht, ist zuständig.

Die folgende Tabelle bietet direkten Teilnehmern, die feststellen möchten, welche Zentralbank für ihr Institut zuständig ist, eine Orientierungshilfe:

Beschreibung der Gegebenheiten	**Zuständige Zentralbank**
Hauptsitz (Zentrale) befindet sich innerhalb/außerhalb[35] des TARGET2-Gebiets; keine Zweigstellen/Töchter.	Zentralbank, die eine Rechtsbeziehung mit der Zentrale hat.
Hauptsitz (Zentrale) und Zweigstellen/Töchter befinden sich innerhalb/außerhalb des TARGET2-Gebiets; beide sind direkte Teilnehmer, und das Routing des Zahlungsverkehrs nach TARGET2 erfolgt über die technische Infrastruktur der Zentrale.	Zentralbank, die eine Rechtsbeziehung mit der Zentrale hat.
Hauptsitz (Zentrale) und Zweigstellen/Töchter befinden sich innerhalb/außerhalb des TARGET2-Gebiets; beide sind direkte Teilnehmer, verfügen jedoch über ihre eigene technische Infrastruktur für das Routing von Zahlungen zu TARGET2.	Jeweilige Zentralbank, die eine Rechtsbeziehung mit der Zentrale und den Zweigstellen/Töchtern hat.

[35] Falls die Zentrale nicht im TARGET2-Gebiet ansässig ist, muss sie sich aber innerhalb des EWR befinden.

Es besteht keine Rechtsbeziehung zwischen der innerhalb/außerhalb des TARGET2-Gebiets gelegenen Zentrale und einer TARGET2-Zentralbank, aber das Routing des Zahlungsverkehrs erfolgt über eine Zweigstelle/Tochter, die ein direkter Teilnehmer ist (unabhängig davon, wo die technische Infrastruktur angesiedelt ist).	Zentralbank, die eine Rechtsbeziehung mit der Zweigstelle/Tochter hat.
Serviceprovider, der in keiner Rechtsbeziehung steht (unabhängig davon, ob er sich innerhalb oder außerhalb des TARGET2-Gebiets befindet), unterhält die technische Infrastruktur für Finanzinstitute, die direkte Teilnehmer sind.	Zentralbank, die eine Rechtsbeziehung mit dem Finanzinstitut hat, das betragsmäßig den größten Umsatz über diese technische Infrastruktur nach TARGET2 einliefert.

Tabelle 8: Zuständigkeit der Zentralbank für direkte Teilnehmer

Wie aus der oben stehenden Tabelle hervorgeht, kann in Bezug auf die Servicebüros eine Ausnahmeregelung gelten (siehe den Abschnitt „Servicebüro und Mitglied/Konzentrator“). Denkbar ist eine gemeinsame Nutzung der von einer solchen Institution bereitgestellten technischen Infrastruktur durch einige in verschiedenen Ländern ansässige direkte Teilnehmer (mit geringem Umsatzvolumen). Servicebüros gehen jedoch keine Rechtsbeziehung mit einer Zentralbank ein. Vielmehr stehen sie lediglich mit Kunden in einer Rechtsbeziehung, die ihre technische Infrastruktur zum Routing von Transaktionen nach TARGET2 nutzen. Allerdings sind direkte Teilnehmer, die ein Servicebüro nutzen, aufgrund der Harmonisierten Bedingungen rechtlich verpflichtet, ihre Zentralbank von Ausfällen bei einem solchen Unternehmen in Kenntnis zu setzen.[36] In einem solchen Fall und um die Erhebung von identischen Daten über verschiedene direkte Teilnehmer zu vermeiden, obliegt es der Zentralbank, die mit dem betragsmäßig größten direkten Teilnehmer[37] aller dasselbe Servicebüro nutzenden Teilnehmer in einer Rechtsbeziehung steht, die Einhaltung der im Rahmenwerk zur Gewährleistung der Sicherheit und operationellen Zuverlässigkeit der Nutzer festgelegten Maßnahmen zu überprüfen (siehe den Abschnitt „Kritische und nichtkritische Teilnehmer“).

Wenn die direkten Teilnehmer ein Mitglied/einen Konzentrator nutzen[38], gibt es zwei Möglichkeiten: Entweder ist das Mitglied/der Konzentrator selbst ein direkter Teilnehmer, dann übernimmt die Zentralbank, die mit diesem direkten Teilnehmer in einer Rechtsbeziehung steht, die in diesem

36 Harmonisierte Bedingungen, Artikel 28 Absatz 2: „Die Teilnehmer informieren die [zuständige Zentralbank] über alle sicherheitsrelevanten Vorfälle in ihrer technischen Infrastruktur und, sofern dies angemessen erscheint, über sicherheitsrelevante Vorfälle in der technischen Infrastruktur von Drittanbietern.“

37 Welcher unter diesen direkten Teilnehmern der größte ist, kann sich ändern, beispielsweise im Zuge einer Fusion. In einem solchen Fall muss die weitere Vorgehensweise geprüft werden.

38 Gleiches gilt, wenn die TARGET2-Nutzer andere Vereinbarungen für die gemeinsame Nutzung von IT-Infrastruktur treffen, z. B. durch die Auslagerung der Zahlungsabwicklung an ein darauf spezialisiertes Unternehmen (in einigen Fällen ein Joint Venture mit anderen TARGET2-Nutzern).

Leitfaden beschriebenen Zuständigkeiten; oder das Mitglied/der Konzentrator ist lediglich ein Verbindungsdienstleister (der nicht in einer Rechtsbeziehung mit einer Zentralbank steht); in diesem Fall ist die Zentralbank, die mit dem betragsmäßig größten, dasselbe Mitglied/denselben Konzentrator nutzenden direkten Teilnehmer in einer Rechtsbeziehung steht, für die Überprüfung der Einhaltung der relevanten Sicherheitsanforderungen zuständig.

Um eine effektive Durchführung dieser Tests zu gewährleisten, müssen die direkten Teilnehmer ihrer Zentralbank auf Anfrage die notwendigen Informationen und Dokumente zur Verfügung stellen.

Jede entdeckte Schwachstelle muss auf der Grundlage eines harmonisierten Ansatzes genau untersucht werden. Anschließend muss die weitere Vorgehensweise zur Beseitigung dieser Schwachstellen abgestimmt und die Umsetzung der beschlossenen Maßnahmen überwacht werden. Diese Aufgabe fällt ebenfalls in den Zuständigkeitsbereich der Zentralbanken.

Schließlich sollten sich die von den Zentralbanken in Verbindung mit diesem Rahmenwerk wahrgenommenen Aufgaben und die von anderen Regulierungsbehörden, z. B. der Bankenaufsicht oder der Zahlungsverkehrsüberwachung, durchgeführten Maßnahmen nicht überschneiden.

3.5.2 Kritische und nichtkritische Teilnehmer

Ungeachtet der zentralen Anforderung, die Wettbewerbsgleichheit zwischen den Nutzern zu gewährleisten, sind sich alle Beteiligten bewusst, dass Sicherheitsmängel, die die Systeme der Finanzinstitute betreffen, je nach wertmäßigem Marktanteil und/oder Art der abgewickelten Transaktionen (z. B. bei Zahlungsvorgängen in systemisch wichtigen Nebensystemen) in ihren Auswirkungen variieren können. Eingedenk dessen ist zwischen *kritischen Teilnehmern* und *nichtkritischen Teilnehmern* zu unterscheiden.[39]

Es steht eine Reihe grundlegender Instrumente zur Verfügung, die sowohl auf kritische als auch auf nichtkritische Teilnehmer anwendbar sind. Damit der entscheidenden Bedeutung der kritischen Teilnehmer für das reibungslose Funktionieren des TARGET2-Systems Rechnung getragen wird, müssen diese Nutzer jedoch einige zusätzliche Maßnahmen umsetzen.

Im Folgenden werden die TARGET2-Nutzer in Kreditinstitute, Nebensysteme und Servicebüros/Konzentratoren unterteilt. Für jede Gruppe wird erläutert, welche Teilnehmer als kritisch und welche als nichtkritisch gelten.

[39] Dies entspricht auch dem vom EZB-Rat am 31. Mai 2006 verabschiedeten Dokument „Business continuity oversight expectations for systemically important payment systems (SIPS)", worin festgelegt ist, dass kritische Teilnehmer von SIPS-Betreibern als solche eingestuft werden.

3.5.2.1 Kreditinstitute

Allgemeine Überlegungen und Grundsätze

Bei der Festlegung der Bestimmungskriterien für die Einstufung eines Kreditinstituts als kritisch oder nichtkritisch gilt der Grundsatz, dass neben den Instituten mit einem ausreichenden betragsmäßigen Marktanteil auch solche als kritisch gelten, bei denen ein Ausfall bei der Erfüllung ihrer Verpflichtungen dazu führen könnte, dass auch andere Teilnehmer oder Finanzinstitute in anderen Bereichen des Finanzsystems nicht mehr in der Lage sind, ihren Verpflichtungen bei Fälligkeit nachzukommen.[40] Dies bedeutet insbesondere, dass eine Betriebsstörung[41] zu einer Liquiditätsansammlung auf dem Konto eines TARGET2-Nutzers führen könnte, die wiederum die Ausführung von Zahlungen durch andere Systemnutzer verhindern und eventuell systemische Risiken verursachen könnte.

Bestimmungskriterien

Die Festlegung von Kriterien zur Unterscheidung zwischen kritischen und nichtkritischen Kreditinstituten sollte logischerweise vom betragsmäßigen Anteil des jeweiligen Kreditinstituts am Gesamtumsatz abhängen.

Das Eurosystem betrachtet ein Kreditinstitut grundsätzlich als kritischen TARGET2-Teilnehmer, wenn es im ersten Jahresquartal im arbeitstäglichen Durchschnitt betragsmäßig mindestens 1 % des TARGET2-Umsatzes abwickelt[42] (ausgenommen Transaktionen, die von Dritten, z. B. Nebensystemen, vorgenommen werden, Zahlungen, die über MT 204 ausgeführt werden, und Übertragungen zwischen den Konten desselben Teilnehmers).

Dieses Kriterium wird regelmäßig überprüft. Anhand der in Abschnitt 3.5.8 beschriebenen Überprüfungsklausel wird gewährleistet, dass das Kriterium im Sinne der beim Betrieb des TARGET2-Systems gewonnenen Erfahrungen an die Geschäftspraxis angepasst wird.

Möglicherweise nutzen zwei oder mehr Kreditinstitute die technische Infrastruktur für die Teilnahme am TARGET2-System gemeinsam. Wenn der Gesamtwert der von diesen Kreditinstituten im gemeinsamen Umfeld abgewickelten Transaktionen betragsmäßig gleich oder größer als 1 % ist, wird

40 Prinzipien für Finanzmarktinfrastrukturen (Principles for Financial Market Infrastructures), Bank für Internationalen Zahlungsausgleich, April 2012.

41 Im Gegensatz zu Bilanzproblemen.

42 Der TARGET2-Umsatz beinhaltet auch Übertragungen an/von Geldkonten, nicht aber die Abwicklung von Wertpapieren (z. B. Lieferung gegen Zahlung (L/Z).

die Organisation, die die Infrastruktur im rechtlichen Sinne betreibt (z. B. eine Transaktionsbank), als kritischer Teilnehmer klassifiziert.

Zu beachten ist, dass die Zentralbanken zusätzlich zu dem oben genannten, vom Eurosystem gemeinsam vereinbarten Hauptkriterium bei der Einstufung der Kreditinstitute, mit denen sie eine Geschäftsbeziehung unterhalten, spezifische nationale Besonderheiten berücksichtigen können. Infolgedessen können die Zentralbanken sogar vorschlagen, direkte Teilnehmer als kritisch einzustufen, die dieses Hauptkriterium nicht erfüllen. Die betreffende Zentralbank muss die EZB über diese Neuklassifizierung informieren und die Gründe dafür erläutern. Die EZB wird dann eine Stellungnahme darüber abgeben, ob die Neuklassifizierung angemessen ist.

Um Neuklassifizierungsanträge anhand messbarer Kriterien beurteilen zu können, werden Simulationstechniken angewandt[43]. Im Einzelnen werden dabei ein technischer Ausfall des Kreditinstituts simuliert und die Auswirkungen, die dieser Ausfall auf die Abwicklung von TARGET2-Zahlungen haben könnte, gemessen. Allgemein gilt, dass ein Kreditinstitut (wieder) als kritischer Teilnehmer eingestuft werden kann, wenn die Simulation ergibt, dass im Schnitt 1,5 % des gesamten TARGET2-Umsatzes aufgrund des Ausfalls der technischen Infrastruktur dieses Kreditinstituts nicht abgewickelt werden konnten[44].

Die von der EZB abgegebene Stellungnahme wird dem betreffenden Gremium[45] des Eurosystems zur weiteren Prüfung vorgelegt. Schließlich ist noch zu erwähnen, dass ein direkter Teilnehmer, der das Hauptkriterium erfüllt, von den Zentralbanken nicht als nichtkritischer Teilnehmer eingestuft werden kann.

3.5.2.2 Nebensysteme

Die Gruppe der Nebensysteme setzt sich aus Organisationen/Institutionen aus dem Bereich Wertpapierverrechnung und -abwicklung, Massenzahlungsverkehrssysteme - systemrelevante Massenzahlungsverkehrssysteme (Systemically Important Retail Payment Systems - SIRPS), besonders bedeutsame Massenzahlungsverkehrssysteme (Prominently Important Retail Payment

43 Für die Simulationen wird der TARGET2-Simulator verwendet, der von der finnischen Zentralbank in Zusammenarbeit mit den 3ZB entwickelt wurde. Weitere Informationen zum TARGET2-Simulator sind dem TARGET-Newsletter (Ausgabe 7, Q4 2013, abrufbar unter www.target2.eu) zu entnehmen.

44 Bei Teilnehmern, die die obige Schwelle von 1,5 % überschreiten und nicht als kritisch eingestuft wurden, wird eine Neuklassifizierung durchgeführt, es sei denn, die Zentralbank des Teilnehmers legt anderweitige Nachweise vor.

45 Dabei handelt es sich um das Komitee für Zahlungs- und Verrechnungssysteme (PSSC), welches die Beschlussorgane des Eurosystems bei der Erfüllung der grundlegenden Aufgaben des ESZB unterstützt, insbesondere bei der Förderung des reibungslosen Betriebs der Zahlungssysteme.

Systems - PIRPS) und andere Massenzahlungsverkehrssysteme - sowie sonstigen Großbetragszahlungssystemen (z. B. CLS und EURO1) zusammen.

Wie bei den Kreditinstituten gibt es bei den Nebensystemen keine empirischen Belege für die genauen Ursachen von systemischen Risiken. Deshalb wurden die Kriterien zur Einstufung der Nebensysteme anhand der Ergebnisse einer Konsultation der betreffenden Stellen des Eurosystems und der verfügbaren Dokumente festgelegt.

Massen- und Großbetragszahlungssysteme

Großbetragszahlungssysteme werden per Definition als systemrelevant klassifiziert. Da durch eine Nichtabwicklung von Zahlungen für diese Systeme über TARGET2 Schocks innerhalb des gesamten Finanzsystems (und im Fall von CLS sogar weltweit) übertragen werden könnten, werden diese Systeme als kritische Teilnehmer eingestuft.

Aus demselben Grund werden SIRPS, die über TARGET2 abwickeln, ebenfalls als kritische Teilnehmer klassifiziert.

Was PIRPS und andere Massenzahlungssysteme anbelangt, so ist davon auszugehen, dass es keine systemischen Auswirkungen für das TARGET2-System oder seine Teilnehmer hätte, wenn die Salden nicht mit Zentralbankgeld ausgeglichen würden. Daher werden diese Systeme als nichtkritische Teilnehmer eingestuft.

Organisationen/Institutionen aus dem Bereich Wertpapierverrechnung und -abwicklung

Organisationen/Institutionen aus dem Bereich Wertpapierverrechnung und -abwicklung sind Zentralverwahrer (Central Securities Depositories - CSDs), internationale Zentralverwahrer (International Central Securities Depositories - ICSDs) und zentrale Kontrahenten (Central Counterparties - CCPs).

Nach Auffassung des Eurosystems haben alle diese Systeme systemische Bedeutung, und der Ausfall eines (I)CSD/CCP würde sich gravierend auf das reibungslose Funktionieren von TARGET2 auswirken. Demzufolge gelten alle Organisationen/Institutionen aus dem Bereich Wertpapierverrechnung und -abwicklung als kritische Teilnehmer.

Zur Vermeidung einer Überregulierung muss die betreffende Zentralbank eventuell von Fall zu Fall prüfen, ob eine bestimmte Organisation/Institution aus diesem Bereich tatsächlich als kritischer Teilnehmer eingestuft werden sollte. Würde sich dabei herausstellen, dass der Ausfall einer solchen Organisation/Institution keine systemischen Auswirkungen für das TARGET2-System oder seine Teilnehmer hätte, könnte die betreffende Zentralbank diese als nichtkritischen Teilnehmer

klassifizieren. Die betreffende Zentralbank muss die EZB über diese Neuklassifizierung informieren und die Gründe dafür erläutern. Die EZB wird dann eine Stellungnahme darüber abgeben, ob die Neuklassifizierung angemessen ist. Dieser kann beschließen, dass die von der Zentralbank zur Neuklassifizierung angewandten Kriterien allgemein zugrunde gelegt werden sollen.

3.5.2.3 „Servicebüro“ und „Mitglied/Konzentrator“

Neben der gemeinsamen Nutzung der SWIFTNet-Verbindung eines anderen SWIFT-Kunden bestehen für einen TARGET2-Nutzer zwei weitere Möglichkeiten, sich indirekt[46] mit SWIFTNet zu verbinden:

- Auslagerung des Tagesgeschäfts an einen Dritten, ein sogenanntes „Servicebüro“[47]
- Inanspruchnahme eines „Mitglieds/Konzentrators“ (neben der technischen Anbindung im vorherigen Punkt), das/der zusätzliche Dienstleistungen anbietet, z. B. die Übernahme der SWIFT-Administration und die Rechnungsstellung im Namen des Nutzers.

Kreditinstitute und eventuell auch Nebensysteme können beschließen, eines dieser Verbindungsmodelle zu nutzen. Sie erhalten einen BIC8 für die Adressierung über SWIFT und übernehmen die Verantwortung für ihre Nachrichten, weshalb sie als direkte Teilnehmer eingestuft werden, obgleich sie nur indirekt verbunden sind. Da das Routing des Zahlungsverkehrs mehrerer Nutzer über eine indirekte Verbindung erfolgen würde, hätte ein Ausfall der technischen Infrastruktur des Servicebüros oder des Mitglieds/Konzentrators möglicherweise systemische Auswirkungen.

Das Eurosystem hat zwar vorläufig beschlossen, dass Servicebüros zum gegenwärtigen Zeitpunkt nicht per se als kritische Teilnehmer gelten, aber es erscheint ratsam, diese wie kritische Teilnehmer zu behandeln, wenn der gesamte Zahlungsverkehr, dessen Routing über ein solches Unternehmen erfolgt, das 2 %-Kriterium für Kreditinstitute übersteigt.

Da zwischen den Servicebüros sowie den Mitgliedern/Konzentratoren und dem Eurosystem keine Rechtsbeziehung besteht, kann die Rechtsgrundlage für die Erfüllung der in diesem Leitfaden enthaltenen Vorschriften durch solche Unternehmen lediglich über die direkten Teilnehmer hergestellt werden.

---

46 Eine indirekte Verbindung mit SWIFTNet wird in der Regel von kleineren Instituten, die nach einer kostengünstigen SWIFTNet-Connectivity-Lösung suchen, genutzt.

47 Hierbei handelt es sich definitionsgemäß um eine *„non-SWIFT organisation entitled under the SWIFT Service Bureau Policy to provide facilities management and/or data processing services to one or more SWIFT Users, including operation of a SWIFT interface for prime connection to the network and/or for disaster recovery. A Service Bureau may not send or receive messages through the SWIFT network for its own account and accordingly is not entitled to a SWIFT address”* (SWIFT-Glossar, Ausgabe März 2005).

3.5.3 Maßnahmen zur Gewährleistung der Sicherheit und operationellen Zuverlässigkeit von Nutzern

Es gilt der Grundsatz, dass die Maßnahmen zur Gewährleistung der Sicherheit und operationellen Zuverlässigkeit der Nutzer im Verhältnis zu deren Systemrelevanz stehen sollten. In den vorherigen Abschnitten wurden die Kriterien zur Bestimmung kritischer Teilnehmer erläutert. In Abschnitt 3.5.3.1 werden die Maßnahmen beschrieben, die sowohl für kritische als auch für nichtkritische Teilnehmer gelten. In Abschnitt 3.5.3.2 folgen die nur für kritische Teilnehmer anzuwendenden Verfahren.

3.5.3.1 Für kritische und nichtkritische Teilnehmer anzuwendende Maßnahmen

Eine Maßnahme zur generellen Adressierung von Sicherheitsfragen ist die Aufnahme einer Klausel in die zwischen den Zentralbanken und den Nutzern getroffenen rechtlichen Vereinbarungen.

Insbesondere aus Artikel 28 Absatz 1 der Harmonisierten Bedingungen für die Teilnahme an TARGET2 geht klar hervor, dass die Gewährleistung eines angemessenen Schutzes der Vertraulichkeit, Integrität und Verfügbarkeit der Systeme der Nutzer in deren alleiniger Verantwortung liegt.

Zudem legt Artikel 31 Absatz 4 dieser Bedingungen unter anderem fest, dass die Zentralbanken keine Haftung übernehmen, wenn ein Schaden von einem TARGET2-Teilnehmer verursacht wurde. Dies bedeutet, dass der TARGET2-Systembetreiber gegenüber einem TARGET2-Nutzer keinerlei Haftung übernimmt, wenn das reibungslose Funktionieren von TARGET2 aufgrund einer Störung beeinträchtigt wird, die durch eine Fehlfunktion des Systems dieses Nutzers verursacht wurde. Der Nutzer, der das Problem verursacht hat, muss jedoch die Zentralbank entschädigen (gemäß den in den Harmonisierten Bedingungen festgelegten Vorgaben und nach dem jeweils geltenden Recht), wenn diese aufgrund der Störung andere Nutzer schadlos halten musste.

Monitoring und Störungsberichte

Für das reibungslose Funktionieren des TARGET2-Systems ist von entscheidender Bedeutung, dass ein Nutzer in der Lage ist, eine Kumulierung von Liquidität auf seinem Konto zu verhindern. Deshalb sind das Monitoring der Verfügbarkeit einer TARGET2-Komponente sowie Störungsberichte zwei Maßnahmen, die - längerfristig - zur Stabilität und Sicherheit des TARGET2-Systems beitragen können.

Sobald ein Nutzer am System teilnimmt, unterliegt er dem Monitoring[48] der zuständigen Zentralbank. Ist ein Nutzer von einer Störung betroffen, sind die zuständigen Mitarbeiter angehalten, die betreffende Zentralbank auf eigene Initiative unverzüglich zu informieren. Sobald der Nutzer den Betrieb wieder aufgenommen hat, kann ihm die Zentralbank ein Formular für einen Störungsbericht (Anhang II) zukommen lassen. In diesem Bericht muss der Nutzer die grundlegende Ursache des Problems, die Auswirkungen, die Schritte, die zur Lösung unternommen wurden, sowie die Maßnahmen, die ein erneutes Auftreten der Störung verhindern sollen, beschreiben.

Eine kleinere Betriebsstörung kann zwar zu Schwierigkeiten bei der Zahlungsabwicklung führen, gilt aber als unbedenklich, wenn sie bei kritischen Teilnehmern nicht länger als 30 Minuten dauert[49]. Solange die Dauer einer Störung diesen Zeitraum nicht überschreitet, ist kein Störungsbericht erforderlich. Bei nichtkritischen Teilnehmern entscheidet die betreffende Zentralbank, ob ein solcher Bericht benötigt wird. Hierbei ist ausschlaggebend, ob die Störung Auswirkungen auf das reibungslose Funktionieren von TARGET2 oder auf andere Nutzer hatte. In diesem Zusammenhang ist anzumerken, dass kein Störungsbericht erforderlich ist, wenn ein Nutzer bewusst beschließt, die Zahlungsabwicklung für einen bestimmten Zeitraum auszusetzen, obgleich es keine technischen Probleme gibt. Um Irritationen zu vermeiden, ist der Nutzer gehalten, seine jeweilige Zentralbank so bald wie möglich über die Aussetzung zu informieren.

Wie oben erwähnt wird kein formeller Störungsbericht benötigt, wenn die Betriebsstörung nicht länger als 30 Minuten dauert oder eine bewusste Entscheidung, die Zahlungsabwicklung auszusetzen, getroffen wurde. Beobachtet eine Zentralbank jedoch wiederholt kurze Betriebsstörungen, setzt sie sich mit ihrem Nutzer in Verbindung und bittet diesen um Klärung, was letztendlich eine formelle Stellungnahme erforderlich machen könnte.

Die Nutzer müssen den ausgefüllten Störungsbericht innerhalb von zwei Geschäftstagen nach Auftreten der Störung an die betreffende Zentralbank zurücksenden. Es gibt zwei Arten von Störungsberichten:

- Wenn die Störung zu diesem Zeitpunkt bereits ausgewertet wurde, wird der erste Störungsbericht als abschließender Auswertungsbericht erachtet.
- Wenn die Störung noch untersucht wird, sollten die ursprünglichen Informationen, die bereits zur Verfügung gestellt werden können, als Zwischenbericht betrachtet werden. Der abschließende

48 Grundprinzip VII (7.7.4): *Die Systembetreiber sollten auch die „Sicherheit und Zuverlässigkeit der Teilnehmer (...) überwachen, z. B. die Verfügbarkeit ihrer Komponenten während der üblichen Geschäftszeiten“*.

49 Berechnet ab dem Zeitpunkt, an dem die Störung bemerkt wurde, bis zur erneuten Betriebsbereitschaft des Systems.

Auswertungsbericht**,** der die im Zwischenbericht enthaltenen Informationen vervollständigt, sollte dann spätestens einen Monat nach Auftreten der Störung an die Zentralbank geschickt werden.

Sobald der Störungsbericht abgeschlossen ist, wird er überprüft, analysiert und in einer Störungsübersicht vermerkt. Birgt das Verhalten eines Nutzers Risiken für das reibungslose Funktionieren von TARGET2 oder andere Nutzer, müssen angemessene Maßnahmen ergriffen werden; beispielsweise sollte die Führungsebene des Nutzers auf das Problem aufmerksam gemacht werden.

Störungen, die die Verfügbarkeit des Nutzers betreffen, sind wahrscheinlich die einzigen, die vom Systembetreiber selbst erkannt werden können, indem dieser die gegenwärtige Zahlungsabwicklung mit dem normalen Verlaufsmuster vergleicht. Bemerkt eine Zentralbank eine Abweichung vom normalen Verlauf und vermutet, dass der Nutzer möglicherweise schwerwiegende Probleme hinsichtlich der Verfügbarkeit hat, über die sie nicht informiert wurde, wird der betreffende Nutzer kontaktiert und um eine Erklärung gebeten.

Darüber hinaus werden die Nutzer dazu aufgefordert, die Vertraulichkeit und Integrität betreffende Sicherheitsprobleme auf eigene Initiative zu melden. Werden Informationen über solche Probleme öffentlich gemacht, könnte sich dies negativ auf die Reputation des gesamten TARGET2-Systems auswirken. Nur wenn der Systembetreiber von solchen Störungen Kenntnis erlangt, kann sichergestellt werden, dass eine geeignete Kommunikationsstrategie zur Beruhigung der Finanzmärkte und der Öffentlichkeit angewandt wird.

3.5.3.2 Nur für kritische Teilnehmer anzuwendende Maßnahmen

Systemsicherheit im Einklang mit Standards

Das Prinzip 17 der Prinzipien für Finanzmarktinfrastrukturen (Principles for Financial Market Infrastructures - PFMI), die vom Ausschuss für Zahlungsverkehrs- und Abrechnungssysteme (Committee on Payment and Settlement Systems - CPSS) und der Internationalen Organisation der Wertpapieraufsichtsbehörden (International Organization of Securities Commissions - IOSCO) herausgegeben wurden (im Folgenden als „PFMI“ bezeichnet), besagt, dass eine Finanzmarktinfrastruktur (FMI) bei der Ausgestaltung ihres Steuerungsrahmens für Betriebsrisiken zahlreiche verschiedene internationale, nationale und branchenspezifische Standards, Richtlinien oder Empfehlungen zugrunde legen kann. Die Einhaltung solcher Geschäftsstandards kann dazu beitragen, ein hohes Maß an Sicherheit und Zuverlässigkeit des Betriebs zu gewährleisten.

Unter Berücksichtigung dessen werden die kritischen Teilnehmer gebeten, selbst zu bescheinigen, dass innerhalb ihres Unternehmens Sicherheitsfragen in Übereinstimmung mit international

anerkannten Standards wie beispielsweise dem Leitfaden für das Informationssicherheits-Management (Code of practice for information security management) (ISO/IEC 27002) adressiert werden. Die Einhaltung anderer Standards, deren Schwerpunkt auf der Informationssicherheit liegt, wäre ebenfalls akzeptabel.

Zu diesem Zweck reicht die für den jeweiligen Bereich zuständige Geschäftsleitung (d. h. die Vorstandsebene oder eine vergleichbare Ebene) des kritischen Teilnehmers bei der betreffenden Zentralbank eine Selbstzertifizierungs-Erklärung[50] ein, aus der hervorgeht, auf welche Weise einer dieser Standards eingehalten werden soll und inwieweit dieser bislang tatsächlich umgesetzt wird. Angesichts der wichtigen Rolle, die der Informationstechnologie (IT) zukommt, muss die Selbstzertifizierung zusätzlich von einem hochrangigen Vertreter aus dem IT-Bereich (auf Vorstandsebene) des kritischen Teilnehmers unterzeichnet werden. Wenn eine Führungskraft des kritischen Teilnehmers sowohl für den Geschäfts- als auch den IT-Bereich zuständig ist, reicht eine Unterschrift aus.

Die Zentralbanken lassen ihren kritischen Teilnehmern das Selbstzertifizierungs-Formular zukommen; diese haben für die Rückantwort drei Monate Zeit. Die Zentralbanken kontrollieren, ob das unterzeichnete Formular vor Ablauf der vorgegebenen Frist zurückgesandt wird. Sollte dies nicht der Fall sein, kontaktieren sie den kritischen Teilnehmer, um die Situation zu klären.

Im Fall der Nichteinhaltung des (selbst festgelegten) Standards, sollte die Selbstzertifizierung ergänzend eine Beschreibung der größten Risiken[51] , die sich aus dieser Situation ergeben, enthalten. Darüber hinaus sollten ein Aktionsplan für die Behebung des Problems sowie Informationen über die für die Umsetzung der einzelnen Maßnahmen vorgesehenen Fristen enthalten sein. Diese Informationen werden ausgewertet, und die Durchführung der Verbesserungsmaßnahmen wird von der zuständigen Zentralbank überwacht.

Business Continuity (Aufrechterhaltung des Geschäftsbetriebs)

Am 31. Mai 2006 verabschiedete der EZB-Rat den Bericht „Business continuity oversight expectations for systemically important payment systems (SIPS)" (im Folgenden „Oversight Expectations"). Es handelt sich dabei um erweiterte Anforderungen der Zahlungsverkehrsüberwachung an die Vorkehrungen zur Aufrechterhaltung des Geschäftsbetriebs von Euro-Zahlungsverkehrssystemen, die für die Stabilität des Finanzsystems von Bedeutung sind.

50 Die Selbstzertifizierungs-Erklärung ist in Anhang III abgebildet.

51 Ein großes Risiko könnten beispielsweise unzureichende Vorkehrungen gegen Denial-of-Service-Angriffe, eine nicht vorhandene unterbrechungsfreie Stromversorgung oder eine ineffektive Vier-Augen-Kontrolle sein.

Die „Oversight Expectations“ enthalten einen Abschnitt, der die Teilnehmer von SIPS betrifft, denn „ein technischer Ausfall der kritischen Systemteilnehmer kann zu systemischen Risiken führen.“ Gemäß diesem Dokument müssen Teilnehmer, die vom Systembetreiber als kritisch eingestuft wurden, bestimmte Mindestanforderungen erfüllen, damit die Aufrechterhaltung des Betriebs im Falle einer Störung sichergestellt ist. Laut den „Oversight Expectations“ obliegt dem Systembetreiber die Verantwortung dafür, die Erfüllung dieser Anforderungen zu überprüfen.

Die kritischen Teilnehmer müssen vor allem bestätigen, dass:

- Business-Continuity-Pläne erstellt werden und Verfahren zu deren Einhaltung verfügbar sind
- ein Ausweichstandort vorhanden ist
- das Risikoprofil des Ausweichstandorts sich von dem des Primärstandortes unterscheidet. Dies bedeutet, dass sich der Ausweichstandort in deutlicher Entfernung vom Primärstandort befinden muss und nicht von denselben Komponenten der physischen Infrastruktur[52] abhängen darf. Dadurch wird das Risiko, dass beide von derselben Störung betroffen sind, minimiert. So sollte beispielsweise der Ausweichstandort an ein anderes Energieversorgungsnetz und eine andere Hauptfernmeldeleitung als der Primärstandort angeschlossen sein[53].

  In diesem Zusammenhang wird berücksichtigt, dass die kritischen Teilnehmer lediglich für Dinge, die in ihren direkten Einflussbereich fallen, verantwortlich sein können. Sie sind zum Teil von den Anbietern abhängig und nicht haftbar, wenn sich die Ausfallsicherheit eines von Dritten bereitgestellten Dienstes als weniger verlässlich erweist als erwartet. Die kritischen Teilnehmer sollten jedoch bestrebt sein, die Festlegung einer angemessenen Ausfallsicherheit in dem mit den Anbietern geschlossenen Vertrag sicherzustellen. So sollte sich z. B. ein Telekommunikationsanbieter im Rahmen der vertraglichen Vereinbarungen verpflichten, mehrere Routing-Einrichtungen bereitzustellen.

- Im Falle einer größeren Betriebsstörung, die dazu führt, dass auf den Primärstandort nicht zugegriffen werden kann und/oder für den Betrieb notwendige Mitarbeiter nicht verfügbar sind, ist der kritische Teilnehmer in der Lage, den normalen Betrieb vom Ausweichstandort aus

52 Zu beachten ist, dass keine Verpflichtung zur Nutzung unterschiedlicher Hardware-Marken und/oder Software-Komponenten besteht, z. B zur Installation von MS Windows am (eigentlichen) Primärstandort und von UNIX-Systemen am Ausweichstandort. Die Aussage „*nicht von denselben Komponenten der physischen Infrastruktur abhängen*“ unterstreicht, dass Ausweichstandorte nicht auf die Infrastrukturkomponenten (z. B. Transport, Telekommunikation, Wasser- und Energieversorgung) angewiesen sein sollten, die am Primärstandort genutzt werden.

53 Basierend auf den „High-level principles for business continuity“, erarbeitet von: The Joint Forum, Bank für Internationalen Zahlungsausgleich, August 2006.

wiederaufzunehmen und so den Geschäftstag ordnungsgemäß abzuschließen und den folgenden Geschäftstag wieder zu beginnen.

- Um die für die Verlagerung vom Primärstandort auf den Ausweichstandort benötigte Zeit zu überbrücken, gibt es Verfahren, die die Durchführung der kritischsten Transaktionen gewährleisten.
- Die Fähigkeit, Störungen zu bewältigen, wird mindestens einmal jährlich geprüft, und wichtige Mitarbeiter werden angemessen geschult.

Die kritischen Teilnehmer sollten im Wege der Selbstzertifizierung erklären, inwieweit sie den „Oversight Expectations" entsprechen. Die Zentralbanken überprüfen dann, ob die „Oversight Expectations" erfüllt werden. Anhand von Tests wird überprüft, ob die zur Aufrechterhaltung des Geschäftsbetriebs getroffenen Vorkehrungen effektiv sind (siehe den Abschnitt „Tests").

Tests

Um zu kontrollieren, ob die Business-Continuity-Maßnahmen wirksam sind, müssen diese regelmäßig getestet werden.

Das Prinzip 17 der PFMI legt fest, dass auch die Systemteilnehmer in die Tests der klar dokumentierten Business-Continuity-Maßnahmen einbezogen werden sollten.

Grundsätzlich können die Tests in zwei Szenarien unterteilt werden. Das erste Szenario beinhaltet die bilaterale Prüfung der zwischen dem kritischen Teilnehmer und seiner Zentralbank vereinbarten Notfallmaßnahmen. Diese Prüfung ist bereits integraler Bestandteil des Test-Programms für Nutzer, das diese vor ihrer Teilnahme an TARGET2 durchlaufen müssen.

Die Teilnahme an den Tests ist für kritische Teilnehmer obligatorisch. Der erfolgreiche Verlauf wird von den betreffenden Zentralbanken überwacht.

Jährliche Erneuerung der Selbstzertifizierung

Systeme, die Informationen wie etwa Zahlungen verarbeiten, agieren in einem sich wandelnden Umfeld. Neue Risiken, neue fachliche Anforderungen oder neu entdeckte Schwachstellen können sich merklich auf die Sicherheit einzelner Systeme auswirken.

Aus diesem Grund benötigt der TARGET2-Systembetreiber eine Rückversicherung, dass die Komponenten der kritischen Teilnehmer weiterhin die vom Eurosystem festgelegten Sicherheitsanforderungen erfüllen. Deshalb werden die kritischen Teilnehmer jährlich aufgefordert zu bescheinigen, dass die Einhaltung der Anforderungen des Eurosystems weiterhin gegeben ist.

In diesem Zusammenhang ist zu erwähnen, dass die jährliche Erneuerung der Selbstzertifizierung nicht mit den technischen Prüfungen zu verwechseln ist, die jeder TARGET2-Nutzer erfolgreich durchlaufen muss, bevor ihm der Anschluss an TARGET2 gestattet wird.

3.5.4 Umsetzung

3.5.4.1 Rechtliche Durchsetzbarkeit

In den Harmonisierten Bedingungen für die Teilnahme an TARGET2, vor allem in Artikel 28 (Sicherheitsanforderungen), werden die Sicherheitsmaßnahmen generell erläutert und somit das Rahmenwerk für die rechtliche Durchsetzbarkeit der in diesem Leitfaden beschriebenen detaillierten Maßnahmen festgelegt. Die praktische und rechtliche Umsetzung, durch die die einzelnen Maßnahmen für Nutzer verbindlich werden, liegt jedoch in der nationalen Zuständigkeit jeder Zentralbank. Demzufolge obliegt es den Zentralbanken zu entscheiden, wie sie die Sicherheitsmaßnahmen für Nutzer in die rechtlichen Vereinbarungen mit ihren Nutzern integrieren (z. B. durch einen Vertragsanhang, eine Veröffentlichung auf der Website mit einem Verweis im Vertrag, ein Schreiben der Zentralbank usw.). Da sich die Gesetzgebung je nach Land unterscheidet und um sicherzustellen, dass die Maßnahmen in allen an TARGET2 teilnehmenden Ländern auf ähnliche Weise und im Einklang mit den Harmonisierten Bedingungen für die TARGET2-Teilnahme rechtlich umgesetzt werden, haben die Zentralbanken darüber Bericht erstattet, auf welche Weise dies erreicht wurde.

3.5.4.2 Übergangsphase

Die Maßnahmen für kritische Teilnehmer definieren die Zugangskriterien, die diese im Idealfall vor der Teilnahme an TARGET2 erfüllen sollten. Neue kritische Teilnehmer müssen selbst bescheinigen, dass die Informationssicherheit im Einklang mit international anerkannten Standards behandelt wird und die im Abschnitt „Business Continuity (Aufrechterhaltung des Geschäftsbetriebs)“ beschriebenen Business-Continuity-Anforderungen erfüllt werden. Darüber hinaus müssten Business-Continuity-Maßnahmen gemäß dem festgelegten Testprogramm (siehe den Abschnitt „Tests“) erfolgreich getestet werden.

Einem kritischen Teilnehmer steht zur Erfüllung der spezifischen Anforderungen hinsichtlich der Sicherheit und der Zuverlässigkeit des Betriebs eine Zeitspanne von 18 Monaten zur Verfügung. Dieser Zeitraum beginnt mit dem Datum seiner Einstufung als kritischer Teilnehmer.

Ferner sollten die betreffenden Zentralbanken einen kritischen Teilnehmer kontaktieren, sobald dieser ermittelt wurde, und ihn bitten, den Stand seiner Vorbereitungen im Hinblick auf die oben

beschriebene Umsetzungsfrist anzugeben. Unterscheidet sich in dieser Einführungsphase die tatsächliche Situation stark von den in diesem Leitfaden erläuterten Anforderungen, sollte ein Arbeitsplan erstellt und dieser von der entsprechenden Zentralbank überwacht werden, damit die erforderlichen Maßnahmen innerhalb der oben erwähnten Frist umgesetzt werden können.

3.5.4.3 Konstruktiver Ansatz

Es sollte ausdrücklich darauf hingewiesen werden, dass das Ziel des Rahmenwerks nicht darin besteht, Kreditinstitute von der Teilnahme an TARGET2 abzuhalten. Die beschriebenen Maßnahmen zielen vielmehr darauf ab, die Ausfallsicherheit und Stabilität des gesamten TARGET2-Systems zu stärken und dadurch zur Stabilität der Finanzmärkte beizutragen.

Wenn ein kritischer Teilnehmer eine der Anforderungen nicht erfüllt, wird die zuständige Zentralbank diesen Teilnehmer auf die aus den festgestellten Schwachstellen resultierenden Risiken hinweisen. In enger Zusammenarbeit mit dem betreffenden kritischen Teilnehmer entwickelt die zuständige Zentralbank ein Programm zur schrittweisen Verbesserung der Situation. Falls eine solche schrittweise Verbesserung durch einen anhaltenden Mangel an Bereitschaft oder in böser Absicht des betreffenden Teilnehmers verhindert wird, sollte der kritische Teilnehmer normalerweise aus dem TARGET2-System ausgeschlossen werden. Eine endgültige Entscheidung hierüber wird aber erst nach eingehender Prüfung der Sachlage auf Eurosystem-Ebene getroffen.

3.5.5 Kommunikation und Koordinierung

Für eine effektive und vertrauensvolle Kommunikation und Koordinierung zwischen den Zentralbanken und ihren Nutzern in Sicherheitsfragen ist eine klare Organisationsstruktur unabdingbar. Es obliegt der Verantwortung aller Zentralbanken und ihrer Nutzer, die ordnungsgemäße und effiziente Durchführung der notwendigen Maßnahmen innerhalb der betreffenden Unternehmen sicherzustellen. Wenn zwischen den beteiligten Parteien sicherheitsempfindliche Informationen ausgetauscht werden, muss gewährleistet sein, dass diese Informationen ordnungsgemäß gekennzeichnet und angemessen geschützt werden.

3.5.6 Vertraulichkeit

Sämtliche von den Nutzern zur Verfügung gestellten Informationen werden vom Eurosystem vertraulich behandelt und lediglich dazu verwendet zu überprüfen, ob die Nutzer die Vorgaben des Eurosystems einhalten, damit dieses seiner Verantwortung als Systembetreiber im Sinne der PFMI gerecht wird.

Falls Nutzer sicherheitsempfindliche Informationen im Zusammenhang mit dem Rahmenwerk erhalten, sind diese selbstredend vertraulich zu behandeln.

3.5.7 Berichterstattung

Die Zentralbanken sind für die Erhebung der erforderlichen Informationen und die Überwachung aller Folgemaßnahmen verantwortlich. Wurden beispielsweise die Vorkehrungen eines Nutzers zur Aufrechterhaltung des Geschäftsbetriebs als ineffektiv eingeschätzt, ist zu erörtern, wie die festgestellten Mängel behoben und bis wann die Abhilfemaßnahmen umgesetzt werden können.

Da das Eurosystem als Ganzes die Verantwortung als Systembetreiber trägt, müssen die von den Zentralbanken gesammelten Informationen über Störungen, die sich auf das reibungslose Funktionieren von TARGET2 auswirken könnten, dem zuständigen Ausschuss auf Eurosystem-Ebene zur Verfügung gestellt werden. Angesichts der Sensibilität der Informationen ist deren streng vertrauliche Behandlung von größter Wichtigkeit. Es könnte sogar in Betracht gezogen werden, die Informationen anonymisiert darzustellen.

Der Ausschuss muss die Informationen prüfen und von Fall zu Fall erwägen, welche Maßnahmen getroffen werden sollten, damit gewährleistet ist, dass ein bestimmter Nutzer kein Risiko für das reibungslose Funktionieren von TARGET2 und für die anderen Nutzer darstellt.

Das Meldeformat und das genaue Verfahren zur Übermittlung von Informationen an den zuständigen Ausschuss werden auf Eurosystem-Ebene festgelegt. Diese internen Verfahren des Eurosystems sollen sicherstellen, dass Zentralbanken, die nicht direkt an der Datenerhebung beteiligt sind, Zugang zu diesen Daten erhalten und die Informationen effektiv und einheitlich ausgetauscht werden.

3.5.8 Überprüfungsklausel

Damit das allgemeine Rahmenwerk weiterhin angemessen bleibt, muss es regelmäßig überprüft werden.

So sind z. B. die zur Bestimmung der kritischen Teilnehmer angewandten Kriterien nicht in Stein gemeißelt. Es obliegt dem Eurosystem, die Kriterien unter Berücksichtigung der während des TARGET2-Betriebs gewonnenen Erfahrungen oder angesichts neuer Forschungsergebnisse zu systemischen Risiken entsprechend anzupassen.

Weiterhin könnte der von einzelnen Kreditinstituten erzeugte Zahlungsverkehr Veränderungen unterliegen. Wenn ein Kreditinstitut nach einer Fusion plötzlich mehr als 1 % des Transaktionswerts über TARGET2 abwickelt, müsste dieses Kreditinstitut als kritischer Teilnehmer eingestuft werden und die für diese Unternehmen festgelegten Anforderungen erfüllen.

Deshalb werden die Kriterien zur Bestimmung kritischer Teilnehmer sowie deren Einstufung mindestens einmal jährlich überprüft. Darüber hinaus sind die Nutzer verpflichtet, die Zentralbanken frühzeitig von wesentlichen Änderungen ihrer Geschäftspraktiken in Kenntnis zu setzen.

3.6 Beendigung oder Suspendierung der Teilnahme eines TARGET2-Teilnehmers

Im Einklang mit der TARGET2-Leitlinie erfolgt eine **fristlose Beendigung oder Suspendierung** der Teilnahme eines Teilnehmers (PM-Kontoinhaber oder DCA-Inhaber) an einem TARGET2-Komponentensystem durch eine Zentralbank ohne vorherige Ankündigung, wenn:

a) ein Insolvenzverfahren über das Vermögen des Teilnehmers eröffnet wird, und/oder

b) der Teilnehmer die Zugangsvoraussetzungen für die Teilnahme am betreffenden Komponentensystem nicht mehr erfüllt.

Die Zentralbank **kann** die Teilnahme eines Teilnehmers an einer TARGET2-Komponente ohne vorherige Ankündigung **beenden oder diesen suspendieren**, wenn:

a) ein oder mehreren Ausfallereignisse (außer den oben genannten) eintreten,

b) der Teilnehmer erheblich gegen die Harmonisierten Bedingungen für die Eröffnung und Unterhaltung eines PM-Kontos oder die Harmonisierten Bedingungen für die Eröffnung und Unterhaltung eines Geldkontos verstößt,

c) der Teilnehmer wesentlichen Pflichten gegenüber der Zentralbank nicht nachkommt,

d) der Teilnehmer aus einer TARGET2 Closed User Group (CUG) oder, im Falle direkt angeschlossener DCA-Inhaber, von einer T2S Closed Group of Users (CGU) ausgeschlossen wird oder dieser aus anderen Gründen nicht mehr angehört,

e) ein anderes Ereignis im Zusammenhang mit einem Teilnehmer eintritt, das nach Ansicht der Zentralbank die Stabilität insgesamt, die Solidität oder die Sicherheit ihrer TARGET2-Komponente oder eines anderen TARGET2-Komponentensystems gefährden oder die Zentralbank in der Erfüllung ihrer Aufgaben, wie sie in den entsprechenden nationalen Gesetzen sowie in der Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank dargelegt sind, beeinträchtigen würde, und/oder unter Risikoerwägungen eine Gefahr darstellt,

f) eine NZB einen Teilnehmer gemäß Anhang III Nummer 12 der TARGET2-Leitlinie vorläufig oder endgültig vom Zugang zu Innertageskrediten ausschließt.

Suspendiert oder beendet eine Zentralbank die Teilnahme eines Teilnehmers an TARGET2, muss sie alle anderen Zentralbanken unverzüglich mittels einer ICM-Nachricht (siehe unten) darüber informieren. Jede Zentralbank hat, sofern sie von einer anderen Zentralbank dazu aufgefordert wird, Informationen bezüglich eines solchen Teilnehmers zur Verfügung zu stellen; dies umfasst im Fall der Beendigung der Teilnahme auch Informationen über an diesen Teilnehmer adressierte Zahlungen.

3.6.1 Auswirkungen der Suspendierung eines PM-Kontoinhabers

- Das PM-Konto und die Unterkonten werden unverzüglich entsprechend gekennzeichnet.
- Die automatische Abwicklung von Zahlungen über diese Konten ist nicht mehr möglich.
- In einem laufenden Abwicklungsprozess (Algorithmus) befindliche Zahlungen sind von der Suspendierung nicht betroffen.
- Die Zentralbank muss Zahlungen in der Warteschlange über das ICM explizit bestätigen, bevor diese über das PM-Konto abgewickelt werden.
- Vom suspendierten PM-Kontoinhaber nach dessen Suspendierung gesendete Zahlungen werden zur Bestätigung durch die Zentralbank über das ICM „geparkt".
- An den suspendierten PM-Kontoinhaber nach dessen Suspendierung gesendete Zahlungen werden zur Bestätigung durch die Zentralbank über das ICM „geparkt".
- Auf welcher Grundlage die Zentralbank die Zahlungen bestätigt, ist von den nationalen Bestimmungen abhängig.

Die **Beendigung der Teilnahme eines PM-Kontoinhabers** führt zur Löschung dieses Teilnehmers aus dem System.

Dabei ist Folgendes zu beachten:

- Was die Vereinbarungen zum Liquiditätspooling betrifft, so tauschen die Zentralbanken, die Vertragspartei einer Vereinbarung über die Aggregierung von Deckungsmitteln (aggregated liquidity - AL) sind und für die PM-Kontoinhaber, die eine solche AL-Vereinbarung geschlossen haben und an ihrer TARGET2-Komponente teilnehmen, als Geschäftspartner fungieren, sämtliche Informationen, die für die Erfüllung ihrer Aufgaben und Pflichten im Rahmen einer AL-Vereinbarung erforderlich sind, aus. Diese Zentralbanken benachrichtigen unverzüglich die leitendende Zentralbank, wenn sie einen Verwertungsfall im Zusammenhang mit der AL-Gruppe oder einem AL-Gruppenmitglied, einschließlich der Zentrale und deren Zweigstellen, bemerken.

- Im Falle der Suspendierung eines PM-Kontoinhabers kann die Zentralbank wählen, ob der suspendierte Teilnehmer weiterhin im TARGET2-Directory veröffentlicht werden soll oder nicht. Aus

dem Eintrag im TARGET2-Directory ist nicht ersichtlich, ob ein PM-Kontoinhaber suspendiert wurde. Die ausführlichen Informationen in den TARGET2-Stammdaten, die über das ICM angezeigt werden können, enthalten jedoch einen entsprechenden Vermerk.

- Handelt es sich bei dem PM-Kontoinhaber, dessen Teilnahme beendet oder suspendiert wurde, um den Leiter einer Kontengruppe, kann dieser ab dem Zeitpunkt, an dem die Beendigung oder Suspendierung wirksam wird, nicht mehr in dieser Funktion auftreten. Ist der suspendierte PM-Kontoinhaber der **Co-Manager** für HAM-Konten, kann er nach der Suspendierung nicht mehr in dieser Funktion agieren. Es obliegt den betroffenen HAM-Kontoinhabern, einen neuen Co-Manager zu benennen.

- Ist der PM-Kontoinhaber, dessen Teilnahme beendet oder suspendiert wurde, ein AS-Verrechnungsinstitut, wird er gemäß den für PM-Kontoinhaber geltenden Regeln behandelt. Die Zentralbank des Verrechnungsinstituts muss die Transaktionen bestätigen.

- Ein vom Zahlungsmodul ausgeschlossenes oder suspendiertes Nebensystem (AS) wird gemäß den für PM-Kontoinhaber geltenden Regeln behandelt. Die Zentralbank des Nebensystems muss die Transaktionen bestätigen.

3.6.2 Auswirkungen der Suspendierung eines DCA-Inhabers

- Das Limit für die Zentralbank-Selbstbesicherung wird auf null gesetzt. Jegliche zuvor gewährte Zentralbank-Selbstbesicherung ist zurückzuzahlen.

- Für das Geldkonto wird eine Innertages-Beschränkung festgelegt, damit keine Verrechnung stattfindet.

- Das PM-Hauptkonto ist nun das PM-Konto der Zentralbank, es sei denn, das PM-Hauptkonto wird von der juristischen Person unterhalten, die auch das Geldkonto unterhält, und wurde ebenfalls suspendiert.

- Die zur Veranlassung von Liquiditätsübertragungen in T2S gewährten Berechtigungen werden widerrufen.

- Vorab festgelegte Aufträge und Daueraufträge für Liquiditätsübertragungen werden gelöscht.

- Die am Tag der Suspendierung auf dem Geldkonto verbleibende Liquidität wird durch den automatisierten Cash Sweep auf das PM-Hauptkonto übertragen.

3.6.3 Auswirkungen der Suspendierung eines HAM-Teilnehmers

- Die Suspendierung wird sofort wirksam.
- Zahlungen können nicht mehr automatisch über die HAM-Konten des Teilnehmers abgewickelt werden.
- Von einem suspendierten Teilnehmer gesendete Zahlungen werden zur Bestätigung durch die Zentralbank „geparkt".
- An einen suspendierten Teilnehmer gesendete Zahlungen werden zur Bestätigung durch die Zentralbank „geparkt".
- Hinsichtlich der Co-Management-Funktion[54] gilt Folgendes: Ist der suspendierte PM-Teilnehmer ein Co-Manager für HAM-Konten, kann er nicht mehr in dieser Funktion agieren, nachdem die Suspendierung wirksam geworden ist. Es obliegt den betroffenen HAM-Kontoinhabern, einen neuen Co-Manager zu benennen. In der Zwischenzeit kann die jeweilige Zentralbank auf Wunsch diese Aufgabe übernehmen. Wird ein HAM-Teilnehmer ausgeschlossen, dessen Konto von einem Co-Manager mit verwaltet wird, so bleibt die Beziehung zwischen dem betreffenden HAM-Kontoinhaber und dem Co-Manager bestehen. Dem HAM-Konto dieses Teilnehmers zu belastende oder gutzuschreibende Transaktionen sind von der Zentralbank auszuführen.

3.7 Vorläufiger oder endgültiger Ausschluss oder Beschränkung des Zugangs zu Innertageskrediten und/oder Selbstbesicherungsfazilitäten

Eine Zentralbank schließt eine Stelle vorläufig oder endgültig von Innertageskrediten/Selbstbesicherungsfazilitäten aus, wenn eines der folgenden Ausfallereignisse eintritt:

a) das Geld- und/oder PM-Konto der Stelle wird vorläufig oder endgültig geschlossen;

b) die betreffende Stelle erfüllt eine der in Anhang III der Harmonisierten Bedingungen für die Eröffnung und Unterhaltung eines PM-Kontos und in den Harmonisierten Bedingungen für die Eröffnung und Unterhaltung eines Geldkontos jeweils festgelegten Anforderungen nicht mehr;

[54] Ein HAM-Konto kann von einem PM-Kontoinhaber mit SWIFT-basiertem Zugang als Co-Manager mit verwaltet werden. Co-Management soll kleinen Banken ermöglichen, ihre Bestände zur Erfüllung der Mindestreservepflicht direkt zu steuern, das Cashflow-Management jedoch an andere Banken zu delegieren.

c) eine zuständige Justiz- oder sonstige Behörde hat die Entscheidung getroffen, ein Verfahren zur Abwicklung der Stelle durchzuführen, einen Insolvenzverwalter oder einen entsprechenden Verantwortlichen für die Stelle einzusetzen oder ein anderes entsprechendes Verfahren einzuleiten;

d) die Gelder der Stelle werden gesperrt und/oder ihr werden andere Maßnahmen von der Europäischen Union auferlegt, die ihre Fähigkeiten beschränken, über ihre Gelder zu verfügen;

e) die Zulassung der Stelle als Geschäftspartner für geldpolitische Geschäfte des Eurosystems wird vorläufig oder endgültig beendet.

Eine Zentralbank kann einen vorläufigen oder endgültigen Ausschluss vom Zugang zu Innertageskrediten vornehmen, wenn sie oder eine andere Zentralbank die Teilnahme des Geldkontoinhabers an TARGET2 suspendiert oder beendet oder ein oder mehrere Ausfallereignisse eintreten.

Beschließt das Eurosystem, den Zugang der Geschäftspartner zu geldpolitischen Instrumenten aufgrund von Risikoerwägungen oder aus sonstigen Gründen gemäß Anhang I, Kapitel 2.4 der Leitlinie EZB/2011/14 vorläufig oder endgültig auszuschließen oder zu beschränken, setzt die Zentralbank diesen Beschluss im Hinblick auf den Zugang zu Innertageskrediten und/oder Selbstbesicherungsfazilitäten gemäß den Bestimmungen der von ihr angewandten vertraglichen Regelungen oder Rechtsvorschriften um.

Die Zentralbank kann beschließen, den Zugang zu Innertageskrediten und/oder Selbstbesicherungsfazilitäten vorläufig oder endgültig auszuschließen oder zu begrenzen, wenn der PM-Kontoinhaber/DCA-Inhaber unter Risikoerwägungen als Gefahr angesehen wird. In solchen Fällen setzt die Zentralbank die EZB und andere Zentralbanken schriftlich hiervon in Kenntnis. Ein solcher Beschluss wird erst mit Zustimmung der EZB wirksam. Sofern es angemessen erscheint, kann der EZB-Rat eine einheitliche Umsetzung der in allen TARGET2-Komponentensystemen ergriffenen Maßnahmen beschließen.

In dringenden Fällen kann Zentralbank den Zugang zu Innertageskrediten und/oder Selbstbesicherungsfazilitäten jedoch mit sofortiger Wirkung vorläufig ausschließen. In solchen Fällen hat die Zentralbank dies der EZB umgehend schriftlich mitzuteilen. Die EZB ist befugt, die Maßnahme der Zentralbank aufzuheben. Wenn die EZB der Zentralbank nicht innerhalb von zehn Geschäftstagen ab dem Zeitpunkt des Zugangs der Mitteilung bei der EZB eine Benachrichtigung über

die Aufhebung der Maßnahme übermittelt, gilt dies als Zustimmung der EZB zu der betreffenden Maßnahme.

Bei Begrenzung von Innertageskrediten ist die Innertageskreditlinie an die Höhe des festgelegten Limits anzupassen. **Bei Innertageskrediten** ist die Innertageskreditlinie auf null zu setzen.

Bei Begrenzung von Selbstbesicherungsfazilitäten ist das Limit für die Zentralbank-Selbstbesicherungsfazilitäten an die Höhe des festgelegten Limits anzupassen. **Bei vorläufiger oder endgültiger Kündigung der Selbstbesicherungsfazilitäten** ist das Limit für die Zentralbank-Selbstbesicherung auf null zu setzen.

3.8 Rechnungsstellung in TARGET2

Die monatliche Rechnung für die in Anspruch genommenen TARGET2-Dienstleistungen wird von der betreffenden Zentralbank zu Beginn des Folgemonats (bis spätestens zum fünften Geschäftstag) an die PM-Kontoinhaber und Nebensysteme geschickt und ist spätestens am zehnten Geschäftstag dieses Monats fällig. Ferner werden allen PM-Kontoinhabern, deren PM-Konto (PM-Hauptkonto) mit einem oder mehreren Geldkonten verbunden ist oder die als T2S-Party definiert wurden, gemäß den Preisvorgaben für T2S auch die Kosten für geldbezogene T2S-Dienstleistungen in Rechnung gestellt.

Nähere Informationen finden sich im DokumentTARGET2 Pricing Guide for Users.

4. Der Geschäftstag im Normalbetrieb

TARGET2-Nutzer sind für die Überwachung ihrer täglichen Operationen auf der Gemeinschafts- und/oder der T2S-Plattform verantwortlich. Parallel dazu kümmern sich die jeweiligen National Service Desks auch um die allgemeine Überwachung des Betriebs im Tagesablauf und um die entsprechenden Bedürfnisse im Bankensektor.

Geeignet für die Durchführung dieser Überwachungsaufgaben sind, was die Dienste auf der Gemeinschaftsplattform (einschließlich TARGET2-Zusatzleistungen) betrifft, das ICM (Informations- und Steuerungsmodul) und wenn es um die Dienste auf der T2S-Plattform geht, die GUI (grafische Benutzeroberfläche).

Im Folgenden werden die Abläufe eines normalen Geschäftstags nach Phasen untergliedert beschrieben. Dabei gilt es zu beachten, dass der Geschäftstag bereits am Abend des vorherigen Werktags beginnt.

4.1 Beginn des Geschäftstags

In TARGET2 (SSP) beginnt der neue Geschäftstag nach erfolgreichem Abschluss der Tagesendearbeiten des vorangegangenen Tages sowie der Vorbereitungsarbeiten für den laufenden Tag (wobei die erste Tätigkeit darin besteht, die Änderungen der Nutzerstammdaten zu laden). Der Wechsel zum neuen Geschäftstag wird in der Regel zwischen 18.45 Uhr und 19.00 Uhr durch eine Broadcast an alle Nutzer bestätigt. Angezeigt werden die Phasen auch auf dem ICM-Bildschirm „SSP Operating Day" unter „Services" – „Administration".

Die ICM-Nachricht lautet wie folgt: „Die Tagesendarbeiten für TT-MM-JJ sind abgeschlossen. Der Geschäftstag TT-MM-JJ ist nun eröffnet."

Das Verfahren zum **T2S-Tagesbeginn** wird ebenfalls um 18.45 Uhr gestartet und dauert bis 20.00 Uhr. Die Bestätigung erfolgt durch eine Statusmeldung zum T2S-Abwicklungstag („Status of the T2S Settlement Day Notification") auf dem GUI-Bildschirm „Daily Schedule" und/oder über „T2S Diary Query". Die Geschäftsanfangsphase beinhaltet die Änderung des Abwicklungsdatums, die Annahme der Datenfeeds von Geldkontoinhabern für die Client Auto-Collateralisation (die bist 19.00 Uhr empfangen werden und für das laufende Abwicklungsdatum gültig sind), die Bewertung der Sicherheiten für die Client-Collateralisation on Stock und die Bewertung der besicherungsfähigen Abwicklungsinstruktionen.

In dieser Phase erfolgt keine Geldverrechnung; sie sollte von den Teilnehmern dazu genutzt werden, die Nachtverarbeitung vorzubereiten.

Kasten 2: Datenfeeds für die Client Auto-Collateralisation

Jeder Geldkontoinhaber, der Client Auto-Collateralisation in T2S anbietet, ist für die Einrichtung und Pflege dieser Selbstbesicherungsfunktion in T2S einschließlich der Konfiguration der erforderlichen Stammdaten verantwortlich. So sollten die folgenden Informationen (Datenfeeds) an T2S übermittelt werden:

- Liste der besicherungsfähigen Wertpapiere für die Selbstbesicherung (nach dem ersten Hochladen sollte sie, wann immer Änderungen vorliegen, aktualisiert werden)
- die täglichen Bewertungen der besicherungsfähigen Wertpapiere

Datenfeeds im Zusammenhang mit der Besicherung (besichtungsfähige Wertpapiere bzw. entsprechende Bewertungen), die für den um 18.45 Uhr beginnenden Abwicklungstag zu verwenden sind, sollten über den ganzen Tag hinweg und idealerweise bis spätestens 17.45 Uhr geliefert werden (wenngleich bis 19.00 Uhr eingehende Informationen noch angenommen werden). Die Bewertungen sollten in Form einer „Flat File" übermittelt werden, während die Liste der notenbankfähigen Wertpapiere gemäß T2S-UDFS[55] per Nachricht bzw. Datei im Format ISO 20022 zu liefern sind.

Kommt es bei der Übermittlung der Bewertungen der besicherungsfähigen Wertpapiere zu Verzögerungen (z. B. wenn die Informationen nicht bis 19.00 Uhr vorliegen), werden die bisher verfügbaren Bewertungen genutzt. Liegen zu den am Vortag geltenden Bewertungen eines bestimmtenbesicherungsfähigen Wertpapiers keine Informationen vor, wird ein Wert von null angesetzt.

Es sei darauf hingewiesen, dass derzeit die T2S-Funktion „Close Links" vom Eurosystem nicht genutzt wird und es daher nicht nötig ist, Informationen zur Liste der „Close Links" zu liefern.

4.2 Liquiditätsbereitstellung

Von 19.00 Uhr bis 19.30 Uhr wird im Bedarfsfall Liquidität für den Zahlungsausgleich während des Tages bzw. der Nacht bereitgestellt. Dabei kann es zu folgenden Liquiditätsbewegungen kommen:

- vom SF auf das PM oder HAM;
- vom HAM oder dem PHA auf das PM.

[55] Die Bereitstellung dieser Information erfordert eine direkte Verbindung zu T2S im A2A-Modus.

Diese 30 Minuten können auch für die Aktualisierung von Kreditlinien oder für die Abwicklung von Repogeschäften vor der Eröffnung genutzt werden.

4.3 Nachtverarbeitung auf der Gemeinschaftsplattform

Liquidität für die Nachtverarbeitung (Dedizierung auf Unter-/Spiegelkonten)

Um 19.30 Uhr erfolgen die Gutschriften auf die Unter- und Spiegelkonten, damit die Nachtverarbeitung der Nebensysteme beginnen kann.

Das Nachtfenster steht von 19.30 Uhr bis 7.00 Uhr zur Verfügung[56] , wobei die Zeit zwischen 22.00 Uhr und 1.00 Uhr als technisches Wartungsfenster für die Gemeinschaftsplattform vorgesehen ist. Auf diese Weise wird die Nachtverarbeitung der unterschiedlichen Nebensysteme in Zentralbankgeld erleichtert. Die in TARGET2 verfügbaren technischen und operationellen Tools ermöglichen eine reibungslose Durchführung der Nachtverarbeitung.

Der Support für an der Nachtverarbeitung teilnehmende Kreditinstitute oder Nebensysteme muss mit der jeweiligen Zentralbank vereinbart werden.

Während des Nachtverarbeitungsfensters können grundsätzlich Liquiditätstransfers mittels ICM zum und vom PM-Konto durchgeführt werden.

Liquiditätsbereitstellung für die Nachtverarbeitung („nicht konkordante Aufträge“)

In der folgenden Abbildung sind die Abläufe des Abwicklungsverfahrens 6[57] dargestellt.

[56] In der Zeit von 6.45 Uhr bis 7.00 Uhr (Beginn der Tagverarbeitung) wird die Öffnung des Tagesbetriebs vorbereitet.

[57] Während der Nachtverarbeitung kann nur das Abwicklungsverfahren 6 verwendet werden. Dennoch könnte das Abwicklungsverfahren 6 sowohl während der Nacht- als auch während der Tagverarbeitung genutzt werden.

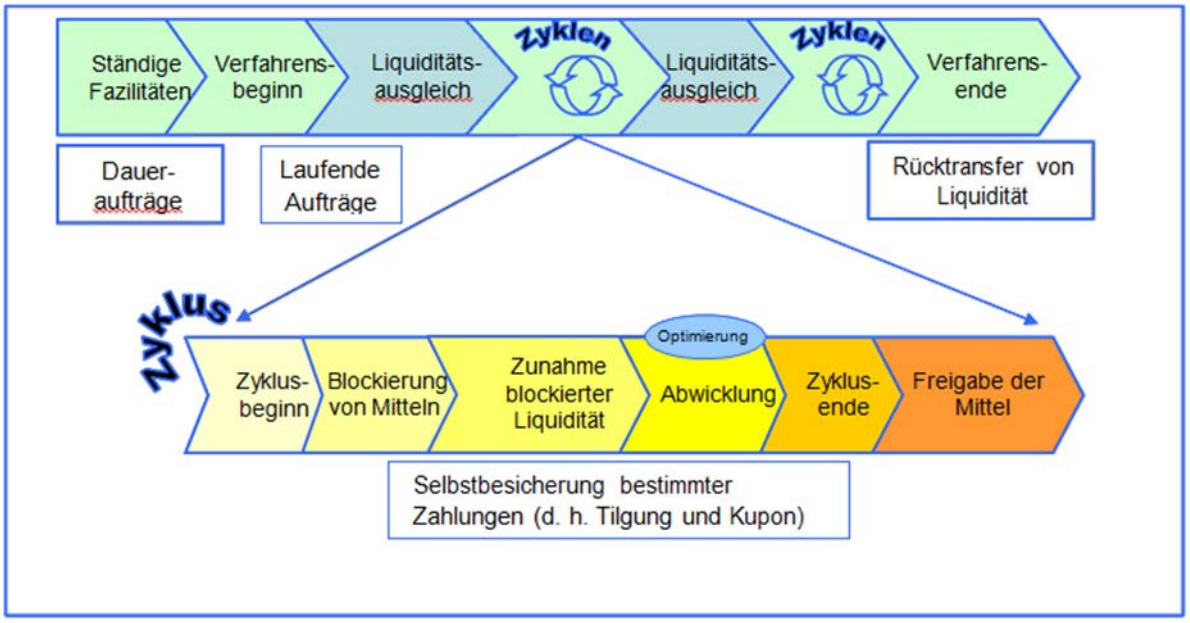


Abbildung 12: Abwicklungsverfahren 6

In diesem Zusammenhang ist zwischen Daueraufträgen und laufenden Aufträgen des PM-Kontoinhabers/der Verrechnungsbank und des Nebensystems zu unterscheiden:

a) Dauerauftrag (nur der Verrechnungsbank)

Der gespeicherte Betrag ist durchgängig bis zur nächsten Änderung maßgebend. Für die Tag- und Nachtverarbeitung können unterschiedliche Aufträge definiert werden. Daueraufträge müssen von der Verrechnungsbank über das ICM bis spätestens 18.00 Uhr eingegeben werden (wirksam ab der nächsten Nachtverarbeitung).

Sie werden unmittelbar nach dem Versand der Nachricht „Beginn des Verfahrens“ („Start-of-procedure“) ausgeführt. Bei unzureichender Liquidität könnte es zu einer Teilausführung kommen. Der verbleibende Teil wird in diesem Fall nicht ausgeführt.

b) Laufender Auftrag („current order“) der Verrechnungsbank

Nach Versand der Nachricht „Beginn des Verfahrens“ („Start of precedure“) – jedoch vor Versand der Nachricht „Ende des Verfahrens“ („End of procedure“) – stellt die Verrechnungsbank per ICM einen laufenden Auftrag ein. Geht er vor dem ersten Zyklus oder zwischen zwei Zyklen (während der Liquiditätsanpassungsphase) ein, wird er sofort ausgeführt. Geht der laufende Auftrag während eines Zyklus ein, wird er zunächst zwischengespeichert. Bei unzureichender Liquidität werden laufende Aufträge zurückgewiesen.

d) Laufender Auftrag („current order“) des Nebensystems

Laufende Aufträge von Nebensystemen unterliegen internen Regelungen. Es bedarf einer Vorabvereinbarung zwischen dem Nebensystem und der Verrechnungsbank. Der Versand laufender Aufträge kann erfolgen, sobald die Nachricht „Beginn des Verfahrens“ verschickt wurde. Geht der laufende Auftrag vor dem ersten Zyklus oder zwischen zwei Zyklen (während der Liquiditätsanpassungsphase) ein, erfolgt eine sofortige Ausführung. Geht er während eines Zyklus ein, wird er zunächst zwischengespeichert. Bei unzureichender Liquidität kommt es zu einer Teilausführung. Der verbleibende Teil wird in diesem Fall nicht ausgeführt.

Konkordanz von Aufträgen

Daueraufträge und laufende Aufträge werden nicht parallel ausgeführt, da Daueraufträge bereits abgewickelt werden, bevor laufende Aufträge versandt werden können.

Unabhängig davon, ob die laufenden Aufträge von einer Verrechnungsbank oder einem Nebensystem erteilt sind, werden sie unmittelbar nach Eingang ausgeführt. Laufende Aufträge, die zunächst zwischengespeichert wurden, weil sie während eines Zyklus eingegangen sind, werden nach dem FIFO-Prinzip ("first in first out"), d. h. in der Reihenfolge ihres Eingangs, ausgeführt.

Bei der Nachtverarbeitung wird für alle teilnehmenden Nebensysteme automatisch eine gemeinsame Nachricht „Beginn des Verfahrens“ verschickt. Dies bedeutet, dass alle Daueraufträge, die eine zu verschiedenen Nebensystemen gehörende Verrechnungsbank erteilt hat, zeitgleich ausgeführt werden. Ist für die Summe der Daueraufträge nicht genügend Liquidität verfügbar, werden alle Daueraufträge anteilig gekürzt. Dies geschieht folgendermaßen:

Ermittlung eines Kürzungsfaktors: Bestehende Liquidität / Summe der Daueraufträge

Kürzung der Daueraufträge: Dauerauftrag x Kürzungsfaktor

4.4 Geldrelevante Aspekte der T2S-Nachtverarbeitung

Während der T2S-Nachtverarbeitung durchlaufen die Liquiditätstransfers – gemäß einer automatischen vordefinierten Reihenfolge namens Sequenz („sequence”) – zwei Abwicklungszyklen. Ein Abwicklungszyklus besteht aus mehr als einer Sequenz.

Liquiditätstransfers von PM-Konten auf Geldkonten und Liquiditätsübertragungen zwischen Geldkonten werden ab Sequenz null (im ersten Nachtverarbeitungszyklus) verarbeitet, d. h., der erste Liquiditätseingang wird gleich zu Beginn der Nachtverarbeitung abgewickelt. Es sei darauf hingewiesen, dass Daueraufträge für Liquiditätstransfers von PM-Konten zu Geldkonten auf der

Gemeinschaftsplattform um 19.30 Uhr und auf der T2S-Plattform um 20.00 Uhr mit dem Start der Sequenz null verarbeitet werden.

Liquiditätstransfers von Geld- auf PM-Konten werden ab Sequenz 1 (im ersten Nachtverarbeitungszyklus) abgewickelt. Liquiditätsübertragungen, die bei einer laufenden Sequenz eingehen, werden in folgenden Sequenzen berücksichtigt.

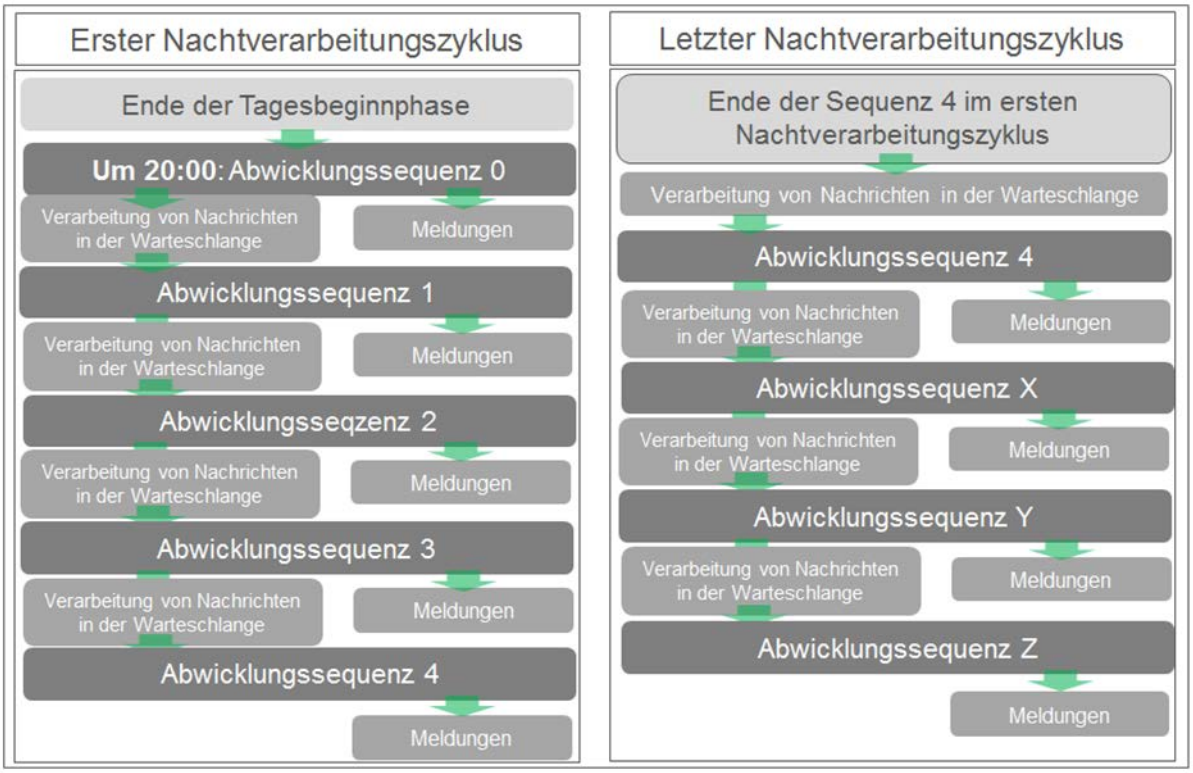


Abbildung 13: T2S-Nachtverarbeitungssequenzen

Am Ende jeder Sequenz generiert T2S vollständige oder Delta-Berichte gemäß Berichtskonfiguration der betreffenden direkt angeschlossenen Geldkontoinhaber. Indirekt angebundenen Geldkontoinhabern werden diese Berichte nicht angeboten.

Wird die Nachtverarbeitung vor 3.00 Uhr abgeschlossen, beginnt die Echtzeitabwicklung vor dem Start des Wartungsfensters (um 3.00 Uhr). Während das Wartungsfenster geöffnet ist, findet in T2S keine Abwicklung statt.

Funktion „Multiple Liquiditätsgeber"

In T2S ist es möglich, dass Geldkontoinhaber Liquidität von verschiedenen PM-Konten erhalten, d. h. von verschiedenen Liquiditätsgebern. Nutzt der Geldkontoinhaber die Funktion „Multiple

Liquiditätsgeber" („multiple liquidity provider"), können die Liquiditätsgeber die erforderlichen Liquiditätsübertragungen auf das Geldkonto veranlassen.

Am Ende der Nachtverarbeitung – in Sequenz Y des letzten Nachtverarbeitungszyklus – wird die restliche Liquidität auf dem Geldkonto automatisch auf die PM-Konten der Liquiditätsgeber – gemäß den Daueraufträgen für Liquiditätstransfers (zur Rückführung der verbleibenden Liquidität auf die PM-Konten) und dem vorab festgelegten Auftrag für die Ausführung dieser Daueraufträge gemäß der Definition in den Stammdaten) – zurückübertragen.

Die Funktion „Multiple Liquiditätsgeber" ist optional und kann nur während der Nachtverarbeitung, in der Sequenz Y des letzten Nachtverarbeitungszyklus verwendet werden.

4.5 Betriebsfenster

Das Eurosystem nutzt dieses Fenster zur Vorbereitung des Tagesgeschäfts.

4.6 SSP-Tagverarbeitung

Um 7.00 Uhr wird TARGET2 für die Verarbeitung von Zahlungsaufträgen geöffnet, was auf dem jeweiligen ICM-Bildschirm angezeigt wird. Die Bestätigung über den störungsfreien Beginn des Tagesbetriebs erfolgt durch eine T2IS-Nachricht.

Während des Tagesbetriebs sollten bestimmte Zahlungsströme aufgrund ihrer systemweiten Bedeutung besonders aufmerksam verfolgt werden. Es wird erwartet, dass die direkten Teilnehmer diese Zahlungen intern vorrangig behandeln.

- 7.00 Uhr – 12.00 Uhr CLS-Zahlungen

Das CLS-System (Continuous Linked Settlement - CLS) ermöglicht die globale Abwicklung von Devisengeschäften in mehreren Währungen, wobei ein Zahlung-gegen-Zahlung-Mechanismus (Payment versus Payment – PvP) Anwendung findet. Zu diesem Zweck hat CLS in jeder zugelassenen Währung Zugang zu Zentralbankgeld. Für die Abwicklung in Euro unterhält CLS ein Konto bei der EZB und nutzt TARGET2, um Euro-Zahlungen zu empfangen und zu versenden. CLS erstellt täglich einen Einzahlungsplan, in dem die Beträge aufgeführt sind, die die Verrechnungsteilnehmer (Settlement-Members) zu fünf Zeitpunkten in stündlichem Abstand (8.00, 9.00, 10.00, 11.00 und 12.00 Uhr) an CLS transferieren müssen. Es steht den Verrechnungsteilnehmern frei, alle ihre Zahlungsverpflichtungen bereits vor diesen Zeitpunkten „in einem Mal" zu erfüllen. Eine Verzögerung bei der Bereitstellung von Euro-Mitteln könnte zu Beeinträchtigungen der Mehrwährungsabwicklung von CLS und womöglich auch der Systeme anderer Währungsräume

führen – insbesondere im asiatisch-pazifischen Raum, wenn dieser wegen des Zeitunterschieds kurz vor Geschäftsschluss steht.

- Zahlungen im Zusammenhang mit dem Margenausgleich für zentrale Kontrahenten (Sicherheitenmargen und Nachschusszahlungen)

Den Beteiligten an Finanzkontrakten, die an einem oder mehreren Märkten gehandelt werden, ist ein zentraler Kontrahent (Central Counterparty – CCP) zwischengeschaltet, der für jeden Verkäufer als Käufer und für jeden Käufer als Verkäufer fungiert.

Ein zentraler Kontrahent kann das Risiko für die Marktteilnehmer insofern erheblich mindern, als er allen Teilnehmern schärfere Risikokontrollmechanismen auferlegt und oftmals auch ein multilaterales Netting der Geschäfte gewährleistet. Ferner erhöht er meist die Liquidität an den von ihm bedienten Märkten, da er für gewöhnlich die Risiken für die Teilnehmer mindert und vielfach den anonymen Handel erleichtert.

Der Margenausgleich für zentrale Kontrahenten erfolgt, indem das Clearinghaus von einem Mitglied zusätzliche Mittel oder Sicherheiten für den Ausgleich von Verlustpositionen auf einem Margenkonto einfordert. Sollten keine Sicherheitenmargen eingehen, verschiebt das Clearinghaus in der Regel den Handelsbeginn am betroffenen Markt. Bleibt die Leistung von Margenzahlungen aus, reichen die möglichen Konsequenzen von der Schließung der Positionen des säumigen Mitglieds bis hin zu dessen Ausschluss.

- 16.08 – 16.45 Uhr EURO1-Zahlungsausgleich

EURO1 ist ein Großbetragszahlungssystem für grenzüberschreitende und inländische auf Euro lautende Transaktionen zwischen Banken, die in der EU operieren. Die Verrechnung erfolgt bei Tagesabschluss über die Nebensystem-Schnittstelle (ASI) mittels Abwicklungsverfahren 4. Gegen 16.08 Uhr wird die Datei zur Durchführung des Zahlungsausgleichs an die ASI gesendet. Der Verrechnungszeitraum endet um 16.45 Uhr. Falls eine Bank ihre Verpflichtungen im Rahmen des EURO1-Zahlungsausgleichs am Tagesende aufgrund von Liquiditätsproblemen nicht erfüllt, wird ein Garantiekonto-Verfahren eingeleitet.

- Abwicklung von Nebensystemen

Die gegenseitigen Abhängigkeiten zwischen TARGET2 und der Abwicklung von Nebensystemen, die nicht unter die vorgenannten Nebensysteme fallen, sowie deren Bedeutungsgrad sind von Land zu Land unterschiedlich und unterliegen der nationalen Zuständigkeit. Daher wird die Frage, in welchem Umfang die Abwicklung von Nebensystemen zu überwachen ist, von den nationalen Zentralbanken selbst geregelt.

- Probleme bei der Verarbeitung

Treten bei der Verarbeitung der oben genannten Geschäftskategorien Schwierigkeiten auf, sollten umgehend Problemlösungsverfahren aktiviert werden. Hier sollten die betroffenen TARGET2-Nutzer zusammen mit den „National Service Desks“ proaktiv handeln.

- 17.00 Uhr: Annahmeschluss für Kundenzahlungen

Um 17.00 Uhr ist Annahmeschluss für Kundenzahlungen. Da Kontobelastungen und -gutschriften zeitgleich erfolgen, gilt Punkt 17.00 Uhr als Annahmeschluss; dies bedeutet, dass Zahlungsaufträge unmittelbar ab diesem Zeitpunkt zurückgewiesen werden. Die Zurückweisung erfolgt nach Ablauf von Algorithmus 3. Der Zeitstempel der Gemeinschaftsplattform ist verbindlich; konkret entscheidet die Uhrzeit, zu der das Modul die Nachricht empfängt. Zentralbanken mit einem PHA-Konto sollten die Konformität mit diesem Annahmeschluss sicherstellen, indem sie beispielsweise frühere Annahmeschlusszeiten ansetzen.

- 18.00 Uhr: Annahmeschluss für Interbankzahlungen

Um 18.00 Uhr ist Annahmeschluss für Interbankzahlungen, aber auch das Ende der Frist für die Zahlungsverarbeitung. Da Kontobelastungen und -gutschriften zeitgleich erfolgen, gilt Punkt 18.00 Uhr als Annahmeschluss; dies bedeutet, dass eingehende Aufträge für Interbankzahlungen unmittelbar nach diesem Zeitpunkt zurückgewiesen werden. Die Zurückweisung erfolgt nach Ablauf von Algorithmus 3. Der Zeitstempel der Gemeinschaftsplattform ist verbindlich; konkret entscheidet die Uhrzeit, zu der das Modul die Nachricht empfängt. Zentralbanken mit PHA-Konten sollten die Erfüllung dieser Ausschlussfrist sicherstellen, indem sie beispielsweise frühere Annahmeschlusszeiten ansetzen.

4.7 Geldrelevante Aspekte der T2S-Nachtverarbeitung

Der Start der T2S-Echtzeitabwicklung (RTS) könnte über eine „Status of the T2S Settlement Day Notification“, einen Eintrag im T2S-GUI-Bildschirm „Daily Schedule” oder eine Nachricht zur Suchanfrage in Verbindung mit „T2S Diary Response” überprüft werden.

Die RTS umfasst:

a) Die **Vorbereitung der Echtzeitverarbeitung**;

b) Zwei **Teilabwicklungsfenster**, von denen das erste von 14.00 Uhr bis 14.15 Uhr und das zweite von 15.45 Uhr und 16.00 Uhr (15 Minuten vor Beginn des DvP-Annahmeschlusses) geöffnet ist. Im Fenster für die Teilabwicklung verarbeitet T2S partiell neue Abwicklungsinstruktionen, die in

T2S eingehen und für eine Teilabwicklung in Frage kommen, sowie bislang unverarbeitete oder nur zum Teil verarbeitete Abwicklungsinstruktionen, die für eine partielle Abwicklung infrage kommen.

c) Schließung der Echtzeitverarbeitung (Real-Time Settlement Closure). Die Schließung der Echtzeitverarbeitungsphase beginnt planmäßig um 16.00 Uhr und umfasst folgende, für die Geldverrechnung äußerst relevanten Verfahren:

Zeit	Ereignisse/Verfahren während des T2S-Abwicklungstags
16.00 Uhr	DvP-Annahmeschluss (nach diesem Annahmeschluss können keine neuen Selbstbesicherungsinstruktionen veranlasst werden)
	Annahmeschluss für Geldverrechnungsrestriktionen („Cash settlement restriction")
	Freigabe nicht genutzter „Cash settlement restriction"
16.30 Uhr	Automatische Erstattung der ZB-Selbstbesicherung
(danach)	Optionales automatisiertes Cash Sweep (falls über Daueraufträge zu Liquiditätsübertragungen konfiguriert)
17.40 Uhr	Annahmeschluss für Abwicklungsinstruktionen für besicherte Geldmarktgeschäfte (Bilaterally Agreed Treasury Management –BATM) und Zentralbankgeschäfte
17.45 Uhr	Annahmeschluss für Liquiditätsübertragungen von PM-Konten auf Geldkonten
(danach)	Automatisierter Liquiditätstransfer (Cash Sweep) zur Übertragung der verbleibenden Liquidität von den Geldkonten auf das entsprechende PM-Hauptkonto. **ANMERKUNG**: Geldkontoinhabern wird empfohlen, die Liquidität von den DCAs auf die PM-Konten frühzeitiger, z. B. vor dem automatisierten Cash Sweep, zu transferieren, um bei Problemen mit diesem Prozess die Liquiditätsrisiken zu begrenzen.
18.00 Uhr	Annahmeschluss für Wertpapierabwicklungsrestriktion sowie Free-of-Payment-Annahmeschluss

Tabelle 9: Abschluss der T2S-Echtzeitabwicklung

Direkt angebundene Geldkontoinhaber können die erwähnten Annahmeschlüsse über den T2S-GUI-Bildschirm „Daily Schedule" und/oder über „T2S Diary Response" Nachrichten zur Suchanfrage überprüfen.

Kasten 3: Automatisierte Rückführung der Zentralbank-Selbstbesicherung

Während der Nachtverarbeitung und auch im Tagbetrieb können Geldkontoinhaber von der Zentralbank-Selbstbesicherung profitieren. Allerdings sind Übernachtkredite auf der T2S-Plattform nicht zulässig, und die Geldkontoinhaber müssen die ZB-Selbstbesicherung daher vor 16.30 Uhr zurückzahlen. Dies sollte über die Freigabe (als CSD-Teilnehmer) der betreffenden Rückführungs-Instruktionen geschehen. Erfolgt dies nicht bis 16.30 Uhr, wird die automatische Rückführung durch die T2S-Plattform ausgelöst. Die Geldkontoinhaber sollten daher die ZB-Selbstbesicherung entweder bis 16.30 Uhr selbst zurückführen oder genügend Liquidität auf dem Geldkonto bereitstellen, um die Rückführung der Selbstbesicherung über das automatische „Auto-Collateralisation Reimbursement" (um 16.30 Uhr) zu ermöglichen.

Dieses Verfahren umfasst die folgenden Schritte, die von der T2S-Plattform automatisch ausgelöst werden:

a) Freigabe der der Instruktionen zur Rückführung der Auto-Collateralisation, die zunächst auf „on hold" gesetzt worden waren

b) Versuch der Abwicklung der noch ausstehenden Rückführungstransaktionen – in Abhängigkeit von der auf dem Geldkonto vorhandenen Liquidität

c) Versuch, die (restlichen) noch ausstehenden Rückführungstransaktionen abzuwickeln – in Abhängigkeit von der auf anderen bei derselben Zentralbank geführten Geldkonten desselben (über BIC11 identifizierten) DCA-Inhabers (z.B. Rebalancing) vorhandenen Liquidität;

d) Umbuchung der Sicherheiten (Collateral relocation) – ein Schritt, über den eine neue Wertpapiertransaktion initiiert wird, um die vom Geldkontoinhaber als Sicherheiten hinterlegten Wertpapiere auf das reguläre Sicherheitenkonto bei der entsprechenden Zentralbank zu transferieren. Nach Erhalt der Information bezüglich dieses Sicherheitentransfers wird die Zentralbank die ZB-Selbstbesicherung in einen Inntertageskredit verwandeln, und zwar auf dem Konto, das vom DCA-Inhaber als Konto für die automatisierte Rückerstattung der ZB-Selbstbesicherung angegeben wird. Dies erfolgt in der Regel über eine verknüpfte Zahlung (connected payment), über die die Zentralbank die Kreditlinie der Gegenpartei erhöht und gleichzeitig das entsprechende Konto belastet.

Eine Strafgebühr von 1.000 EUR wird fällig für jeden Geschäftstag, an dem ein oder mehrere Inanspruchnahmen im Zusammenhang mit dem letzten Schritt der Umbuchung der Sicherheiten erfolgen. Diese Gebühr wird – im Einklang mit den festgelegten nationalen Verfahren – von jeder

Zentralbank erhoben

Anmerkung: *Die in dem entsprechenden PM-Konto registrierte Kreditlinie besteht unabhängig von der Zentralbank-Selbstbesicherung, die im Laufe des Tages an das Geldkonto auf der T2S-Plattform gewährt wurde. Die Kreditlinie wird ihrer Höhe nach durch einen Pool von Sicherheiten unterlegt. Die während des Tages gewährte ZB-Selbstbesicherung wird mit Wertpapieren unterlegt, die zuvor nicht zum Pool gehörten. Erst wenn es der Geschäftspartner versäumt, die Selbstbesicherung bis 16.30 Uhr zurückzuführen, wird die Sicherheit in den regulären Pool umgeschichtet, was zur Ausweitung der Kreditlinie im PM-Konto führt. Um sicherzustellen, dass die höhere Kreditlinie für die Rückerstattung der ZB-Selbstbesicherung verwendet wird, wird die Liquidität aus der Erhöhung der Kreditlinie unmittelbar von dem PM-Konto des Teilnehmers auf das PM-Konto der Zentralbank transferiert. Dies wird in der Regel durch die Nutzung einer „Connected Payment" sichergestellt (in bestimmten Situationen können Zentralbanken von diesem Verfahren abweichen, wenn z. B. eine feste Kreditlinie verwendet wird).*

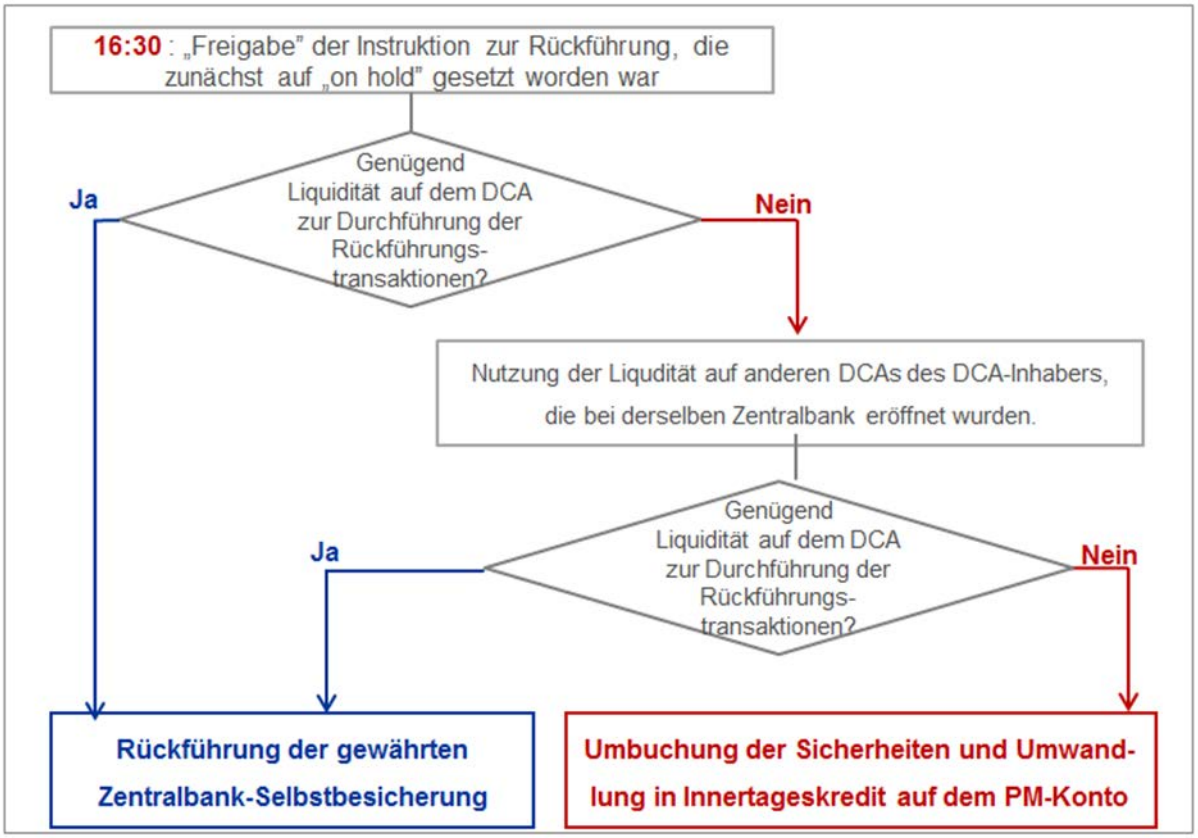

16:30 : „Freigabe" der Instruktion zur Rückführung, die zunächst auf „on hold" gesetzt worden war
Genügend Liquidität auf dem DCA zur Durchführung der Rückführungs-transaktionen?
Ja
Nein
Nutzung der Liquidität auf anderen DCAs des DCA-Inhabers, die bei derselben Zentralbank eröffnet wurden.
Genügend Liquidität auf dem DCA zur Durchführung der Rückführungs-transaktionen?
Ja
Nein
Rückführung der gewährten Zentralbank-Selbstbesicherung
Umbuchung der Sicherheiten und Umwand-lung in Innertageskredit auf dem PM-Konto

Abbildung 14: Automatische Rückführung der Zentralbank-Selbstbesicherung

Es gibt keine automatische Rückerstattung im Falle von Client Auto-Collateralisation.

4.8 Tagesendeverarbeitung

TARGET2 schließt um 18.00 Uhr. Die Schließung der Gemeinschaftsplattform wird durch eine Nachricht im ICM und dem T2IS bestätigt. Die Uhrzeit für den Annahmeschluss wird auch im ICM unter „Services“ – „Administration“ – „SSP Operating Day“ angezeigt. In der Zeit von 18.00 Uhr bis 18.15 Uhr finden folgende Aktivitäten statt:

- Rücktransfer von Liquidität von den Unterkonten auf die Hauptkonten (Contingency-Verfahren)
- Zurückweisung von Zahlungen in der Warteschlange um 18.00 Uhr (unmittelbar nach Ablauf von Algorithmus 3)
- automatisches Verfahren, wenn der Leiter einer Kontengruppe die Konten nicht rechtzeitig ausgleichen konnte und ein Konto der Kontengruppe ohne vorhandene Besicherung in entsprechender Höhe überzogen ist
- automatischer Liquiditätstransfer an das PHA (optional)
- Nutzung der ständigen Fazilitäten bis 18.15 Uhr (bzw. 18.30 Uhr am letzten Tag der Mindesreserve-Erfüllungsperiode)
- automatischer Liquiditätstransfer auf das HAM-Konto (optional)
- Ausgleich der Kontengruppe (Contingency-Verfahren)
- Versand der Saldeninformationen an das RM-Modul
- Senden der Kontonachrichten (MT940/950) an die PM-Kontoinhaber (optional). Nach 18.30 Uhr wird die interne Zentralbankverbuchung vorgenommen.

Was die T2S-Plattform betrifft, so könnte die Ausführung des Tagesend-Prozesses durch direkt angeschlossene Geldkontoinhaber per „Status of the T2S Settlement Day Notification”, über einen Eintrag im GUI-Bildschirm „Daily Schedule” und/oder via „T2S Diary Query” bestätigt werden. Inzwischen generiert T2S alle Tagesschlussberichte und Kontoauszüge auf den Geldkonten – im Einklang mit der Berichtskonfiguration – und sendet sie an die direkt angeschlossenen Geldkontoinhaber. Indirekt angebundene DCA-Inhaber erhalten keine Tagesschlussberichte aus T2S (und insbesondere keine Kontoauszüge).

5. Grundsätzliche Aspekte der Verfahren für Ausnahmesituationen

5.1 Definition einer Störung

Störungen sind Situationen, die den normalen Betrieb von TARGET2 behindern. Solche Situationen können auf Probleme in der Gemeinschaftsplattform, der T2S-Plattform, den PHAs, nationalen Anwendungen, Nebensystemen, bei direkten Teilnehmern und den SWIFT-Diensten zurückzuführen sein.

Eine Störung lässt sich als ein Ereignis definieren, das nicht zum Standardbetrieb gehört und zu einer Unterbrechung oder Einschränkung der von TARGET2 angebotenen Dienstleistungen führt bzw. führen kann. Die Folge könnte unmittelbar oder aber erst in einem späteren Stadium zu sehen und technischer, operationeller oder finanzieller Art sein. Jede Störung muss dokumentiert werden, und es ist so bald wie möglich eine Lösung zu finden und umzusetzen.

Störungen können sich aus einem oder mehreren der folgenden Ereignisse ergeben:

a) dem Ausfall einer wichtigen Komponente bzw. Software in der technischen Plattform des Systems

b) einem verfahrens- oder betriebstechnischen Fehler

c) Streiks oder schwerwiegenden externen Ereignissen (z. B. Naturkatastrophen, großflächige Stromausfälle, Terroranschläge, Koinzidenz von Ereignissen).

Die nachstehende Abbildung zeigt, welche Stellen im Rahmen von TARGET2-Ausnahmesituationen betroffen sein können.

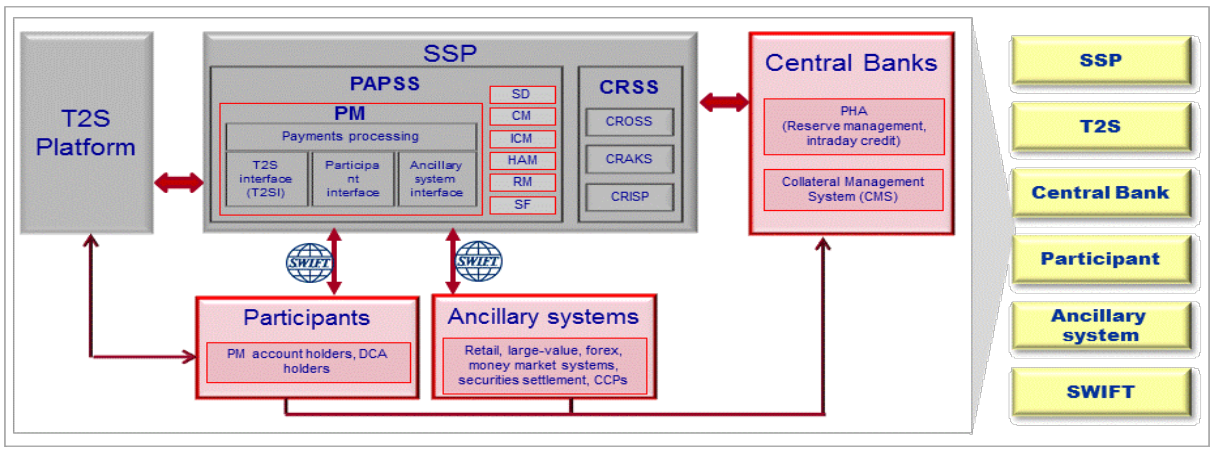


Abbildung 15: Als mögliche Störquellen ermittelte Beteiligte

5.2 Verfahren zur Störungsbehebung

Die Behebung einer Störung beginnt mit der Problemidentifizierung. Die Identifikation von Problemen ist der Hauptzweck des Monitorings der verschiedenen Beteiligten. Sobald eine Abweichung vom Normalbetrieb erkannt und als Problem bestätigt worden ist, werden die Verfahren zur Kommunikation bei Störungen und zur Störungsbehebung eingeleitet. Bei TARGET2 können Probleme entweder von TARGET2-Nutzern oder von den Zentralbanken festgestellt werden.

Allgemein befassen sich die TARGET2-Maßnahmen zur Störungsbehebung mit folgenden Aspekten:

- Lösung/provisorische Lösung des Problems
- Business Continuity, d. h. Aufrechterhaltung der vollen Verarbeitungskapazität durch Umschalten auf ein zweites System/einen zweiten Standort/eine zweite Region
- Contingency-Maßnahmen, die die fortgesetzte Verarbeitung einer begrenzten Anzahl von Zahlungen ermöglichen
- Verschiebung der Annahmeschlusszeit, d. h. Verlängerung der Tagverarbeitung.

Da FIN-Nachrichten sowie InterAct- und FileAct-Dateien durch unterschiedliche SWIFT-Kanäle geleitet werden, könnte die InterAct- und FileAct-Verarbeitung bei einem Ausfall, der lediglich den FIN-Nachrichtenverkehr betrifft, fortgesetzt werden, wodurch die Abwicklung (sehr) kritischer Zahlungen möglich wäre.

5.3 Kommunikation bei Störungen

In Ausnahmesituationen ist der Informationsfluss von entscheidender Bedeutung. Bei Störungen halten die TARGET2-Nutzer über nationale Kommunikationswege mit ihren üblichen für das Betriebsmanagement zuständigen Ansprechpartnern in der jeweiligen Zentralbank Kontakt.

Störungen mit möglichen systemischen Auswirkungen unterliegen einem koordinierten Management durch die Zentralbanken. Darüber hinaus gibt es bei den Zentralbanken eine interne Struktur für den Umgang mit TARGET2-Störungen, die zusätzlich zur normalen Organisationsstruktur eingesetzt wird.

Informationsbereitstellung bei Ausfällen

Bemerken die Zentralbanken einen Ausfall der Gemeinschaftsplattform oder andere Ausfälle, die sich auf die Abwicklung von TARGET2-Transaktionen auswirken könnten, aktivieren sie ihre internen, über fest etablierte Telekonferenzsysteme laufenden Kommunikationswege für den Störungsfall. Nach der Festlegung des weiteren Vorgehens werden Informationen über die in Abschnitt 2.4.1 erläuterten Kommunikationsmittel gleichzeitig an alle TARGET2-Nutzer geleitet.

Um eine zeitnahe Kommunikation zu gewährleisten, bestehen die Mitteilungen aus im Voraus vereinbarten, standardisierten Begriffen und enthalten soweit verfügbar folgende Informationen:

a) Beschreibung des Fehlers

b) Erwartete Abwicklungsverzögerung (soweit möglich)

c) Information über die ergriffenen Maßnahmen und

d) Hinweise an die Nutzer.

Sind bei Feststellung einer Störung einige der oben genannten Angaben nicht verfügbar, wird zunächst eine relativ allgemein gehaltene Ankündigung des Vorfalls gemacht. Im weiteren Verlauf, d. h. in der Regel innerhalb von 30 Minuten nach der ersten Ankündigung, werden präzisere Angaben nachgereicht.

Sofern im Verlauf einer Störung weitere für die Nutzer relevante Informationen vorliegen, werden diese über die obigen Kommunikationswege bekannt gegeben. Auf diese Weise werden die Nutzer auch von der Störungsbehebung in Kenntnis gesetzt.

6. Verfahren zur Handhabung von Störungen der Gemeinschaftsplattform

6.1 Verfahren bei Störungen zu Tagesbeginn (18.45 Uhr - 19.00 Uhr)

Der Abschluss des Tagesbeginns wird mit einer Broadcast-Nachricht an alle Nutzer bestätigt. Verzögert sich der Tagesbeginn, wird dies vom betreffenden National Service Desk über nationale Kommunikationswege, das T2IS und gegebenenfalls das ICM mitgeteilt. Eine Verzögerung beim Tagesbeginn kann zu einem verzögerten Start der nachfolgenden Phasen führen und somit die Bereitstellung von Liquidität an die Nebensysteme und die Geldkonten beeinträchtigen.

6.2 Verfahren bei Störungen der Nachtverarbeitung[58] (19.00 Uhr – 22.00 Uhr und 1.00 Uhr – 7.00 Uhr)

Tritt eine Störung der Gemeinschaftsplattform während der Nachtverarbeitung auf, könnte sie sich negativ auf die Liquiditätsbereitstellung, die Nachtverarbeitung, auf die Liquiditätsübertragungen zwischen Geldkonten und PM-Konten und möglicherweise auch auf die Tagverarbeitung auswirken. Ansprechpartner für Nutzer der Nachtverarbeitung wäre auch hier der jeweilige National Service Desk.

Werden Daueraufträge zur Liquiditätsübertragung von PM-Konten zu Geldkonten nicht rechtzeitig und/oder nicht erfolgreich ausgeführt, kann die T2S-Verarbeitung unter ausschließlicher Nutzung der Auto-Collateralisation beginnen . Was die Liquiditätstransfers von den Geldkonten auf die PM-Konten betrifft, so sollten diese bis zur Wiederherstellung der Gemeinschaftsplattform in die Warteschlange gestellt werden. Je nach Art des SSP-Ausfalls besteht die Möglichkeit, das Problem entweder zu beheben oder gegebenenfalls eine Ausfallsicherung in die Wege zu leiten (siehe unten). Von großer Wichtigkeit ist es, zu allen nächtlichen Ereignissen und Maßnahmen, die Implikationen für den Beginn der Tagverarbeitung um 7.00 Uhr haben könnten, umfassende Informationen bereitzustellen. Der „National Service Desk“ wird seine TARGET2-Nutzer daher vor dem regulären Start der Tagverarbeitung um 7.00 Uhr über die nationalen Kommunikationswege und über das T2IS sowie gegebenenfalls per ICM entsprechend informieren.

[58] Keine Verfahren während des Wartungszeitraums (22.00 Uhr - 1.00 Uhr).

6.3 Betriebsfenster (6.45 Uhr - 7.00 Uhr)

Das Eurosystem nutzt das Betriebsfenster zur Vorbereitung der Tagverarbeitung. Bei Störungen gelten die Verfahren zur Störungsbehebung während der Tagverarbeitung.

6.4 Verfahren bei Störungen der Tagverarbeitung (7.00 Uhr - 18.00 Uhr)

6.4.1 Fortsetzung des Geschäftsbetriebs (Business Continuity)

Kann ein SSP-Problem nicht behoben werden, besteht das Hauptziel in der Wiederherstellung der vollen Verarbeitungskapazität. Die Entscheidung, eine Ausfallsicherung durchzuführen, hängt von der Art des Ausfalls, dessen voraussichtlicher Dauer, dem Zeitpunkt usw. ab. Dabei besteht keine definierte Hierarchie mit Blick auf intraregional (innerhalb einer Region) oder interregional (von einer Region zur anderen) zu ergreifende Ausfallsicherungen. Bei Problemen auf der Ebene der Gemeinschaftsplattform ist zu entscheiden, ob die Ausfallsicherung intraregional oder interregional erfolgen muss. Die Aktivierung letzterer Möglichkeit wird nur äußerst selten durchgeführt.

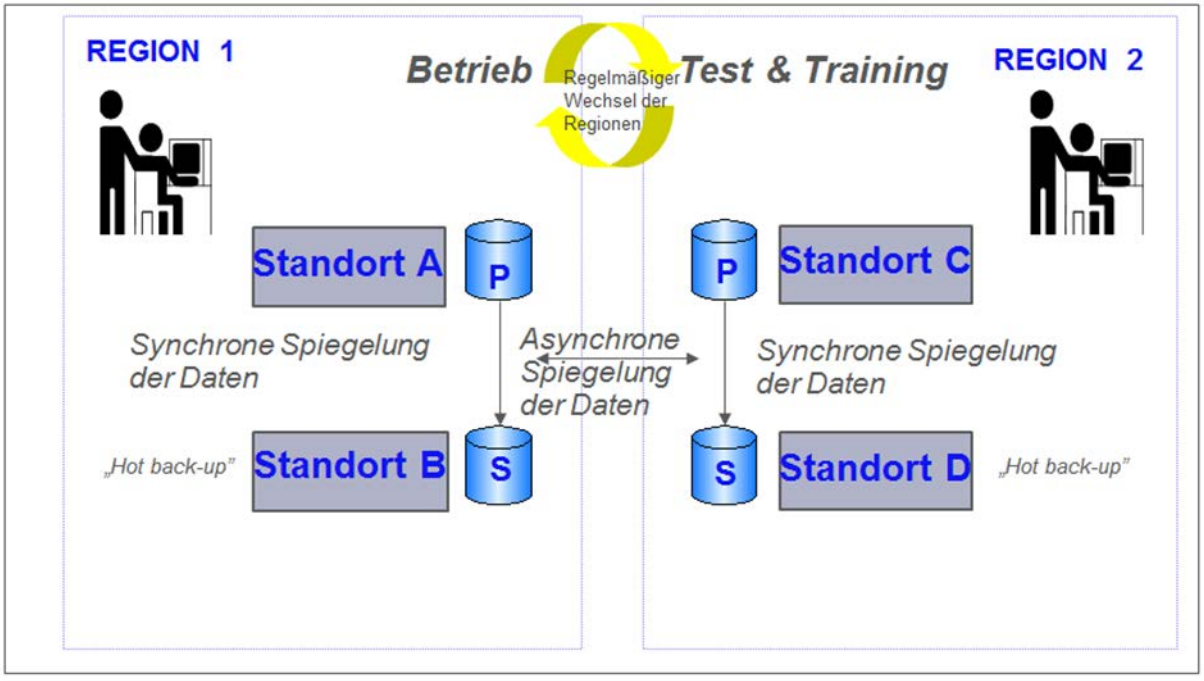


Abbildung 16: Zwei Regionen, vier Standorte

6.4.1.1 Intraregionale Ausfallsicherung

- Während kleinere Ausfälle durch die Sicherung der wichtigsten kritischen Elemente vor Ort aufgefangen werden können, erfordern größere Ausfälle oder Katastrophenfälle (z. B. Störungen wichtiger Hardware durch Brand, Überschwemmung, Terroranschläge oder Fehler in den Telekommunikationsanlagen) die Aktivierung des zweiten Standorts in derselben Region (intraregionale Ausfallsicherung).
- Eine intraregionale Ausfallsicherung bedeutet das Überwechseln von Standort A zu Standort B in ein- und derselben Region. Da im Synchronbetrieb gearbeitet wird, sind die Datenbanken an beiden Standorten auf exakt demselben Stand, weshalb keine Abstimmung nach der Ausfallsicherung erforderlich ist.
- Eine intraregionale Ausfallsicherung gewährleistet die Fortsetzung des normalen Geschäftsbetriebs binnen maximal einer Stunde nach erfolgter Entscheidungsfindung der Zentralbanken.
- Die Zahlungsabwicklung ist während der Ausfallsicherung unterbrochen, doch können die TARGET2-Nutzer weiterhin FIN-Zahlungsaufträge (die auf der SWIFT-Ebene in eine Warteschlange gestellt werden) und FileAct-Nachrichten (im „store & forward mode“) an die Gemeinschaftsplattform senden.

6.4.1.2 Interregionale Ausfallsicherung

- Weitreichende regionale Störungen (z. B. schwerwiegende Verkehrs-, Telekommunikations- oder Stromversorgungsstörungen oder sonstige Beeinträchtigungen kritischer Infrastrukturen, die ein ganzes Ballungsgebiet oder einen geografischen Großraum erfassen) erfordern den Umstieg auf die zweite Region (interregionale Ausfallsicherung).
- Eine interregionale Ausfallsicherung bedeutet das Überwechseln von Region 1 zu Region 2, die in der Regel ein normales Herunterfahren des Standorts in Region 1 ermöglicht. Infolgedessen kann der Betrieb in Region 2 binnen zwei Stunden nach der Entscheidungsfindung ohne Datenverlust wiederaufgenommen werden. Die Nutzer werden informiert, sobald TARGET2 wieder voll zur Verfügung steht.
- Zu einem Datenverlust kann es dank des asynchronen Betriebs nach einer interregionalen Ausfallsicherung lediglich in dem extrem seltenen Fall kommen, dass die beiden Standorte in Region 1 unversehens gleichzeitig ausfallen. In einer solchen Situation bleibt nur die Möglichkeit der Ausfallsicherung auf die Region 2 und der Abstimmung der fehlenden Daten sowie der

Wiederherstellung der Datenbasis. Gleichwohl sollte die Wiederaufnahme des Geschäftsbetriebs in Region 2 einschließlich der Rekonstruierung und Abstimmung der SWIFTNet FIN-Nachrichten[59] binnen zwei Stunden nach der Entscheidungsfindung möglich sein. Der Wiederherstellungsprozess erfordert die aktive Beteiligung der Nutzer. Dieses Verfahren für interregionale Ausfallsicherungen mit Datenverlust, einschließlich des Wiederherstellungsprozesses, wird in Anhang I beschrieben.

- Die Zahlungsabwicklung wird während einer interregionalen Ausfallsicherung unterbrochen. Wenn die Nutzer weiterhin FIN-Zahlungsaufträge senden, so werden diese auf SWIFT-Ebene in eine Warteschlange gestellt und nach Wiederaufnahme des Betriebs der SSP abgewickelt. Dasselbe gilt für Liquiditätsübertragungen an/von Geldkonten, die direkt über T2S oder über die TARGET2-Kern- oder Zusatzleistungen für T2S initiiert wurden und auf Ebene der T2S-Schnittstelle oder der SWIFT-Ebene in die Warteschlange eingestellt werden.

Behandlung von vorab eingereichten Zahlungsaufträgen

➢ Interregionale Ausfallsicherung (ohne Datenverlust)

Ist eine interregionale Ausfallsicherung ohne Datenverlust erfolgt und der hinter dem Codewort angegebene Zeitpunkt verstrichen, so funktioniert die Gemeinschaftsplattform nach den „normalen“ Verfahren. Dies bedeutet:

/FROTIME/ Zahlungen werden in die Verrechnung einbezogen

/TILTIME/ eine Warnmeldung wird im ICM angezeigt

/REJTIME/ Zahlungen werden zurückgewiesen

➢ Interregionale Ausfallsicherung mit Datenverlust

Ist eine interregionale Ausfallsicherung mit Datenverlust verbunden und der hinter dem Codewort angegebene Zeitpunkt verstrichen, arbeitet die Gemeinschaftsplattform nach einem besonderen Verfahren: Zahlungen mit dem Codewort /REJTIME/ werden nicht sofort zurückgewiesen, da die Zeitangabe in einen in der Zukunft liegenden Zeitpunkt umgewandelt wird.

Behandlung von Nebensystem-Transaktionen, für die optionale Dienste genutzt werden

[59] Die Wiederherstellung ist eine von SWIFT angebotene Dienstleistung, die gegenüber den TARGET2-Nutzern nach dem üblichen SWIFT-Gebührenmodell abgerechnet wird.

Abwicklungs-verfahren	Optionaler Dienst	Auswirkungen bei Verstreichen des Zeitpunkts
1.2	festgelegter Abwicklungszeitpunkt („von“)	Abwicklung
	Abwicklungszeitraum („bis“)	Zurückweisung
3	Informationsfrist	Abwicklungsversuch
	Abwicklungszeitraum („bis“)	Zurückweisung
4.5	Informationsfrist	Abwicklungsversuch
	Abwicklungszeitraum („bis“) - ohne Garantieperiode - mit Garantieperiode	Zurückweisung Aktivierung des Garantiekonto-Verfahrens

Tabelle 10: Behandlung von Nebensystem-Transaktionen

Bei einer interregionalen Ausfallsicherung mit Datenverlust verschieben die drei Anbieter-Zentralbanken die Informationsfrist auf 15 Minuten vor dem Annahmeschluss für Kundenzahlungen und verlegen das Ende der Abwicklungszeit auf den Annahmeschluss für Kundenzahlungen, um eine Zurückweisung von Zahlungen nach der Wiedereröffnung der Gemeinschaftsplattform zu vermeiden.

6.4.2 Contingency-Abwicklung unter Einsatz des Contingency-Moduls[60]

Die Contingency-Abwicklung ist eine vorübergehende Maßnahme, bei der nur eine begrenzte Anzahl an Transaktionen abgewickelt wird, um die Entstehung eines systemischen Risikos zu vermeiden. Daher wird das Contingency-Modul (CM) bei Ereignissen eingesetzt, bei denen eine Aufrechterhaltung des Geschäftsbetriebs („Business Continuity“) unmöglich ist oder systemisch wichtige Zahlungen während des Ausfallsicherungsprozesses abgewickelt werden müssen.[61]

Das Konzept der (sehr) kritischen TARGET2-Zahlungen legt fest, welche Zahlungen als systemisch relevant und somit als für die Contingency-Abwicklung zugelassen eingestuft werden. Die Contingency-Abwicklung über das CM ist nur für einige spezielle Überweisungen zwischen Banken möglich. Die Verarbeitung anderer Zahlungen wird verschoben, bis die Gemeinschaftsplattform wieder zur Verfügung steht. In Kasten 4 („Das Konzept (sehr) kritischer TARGET2-Zahlungen“) wird

60 Die Contingency-Abwicklung mithilfe des Contingency-Netzwerks wird in Kapitel 8.5 dargestellt.

61 Der Einsatz des CM hindert die Nebensysteme nicht an der Nutzung ihrer eigenen alternativen Contingency-Mechanismen (z. B. die Hereinnahme zusätzlicher Sicherheiten oder anderer Währungen).

erläutert, für welche Zahlungen die Abwicklung obligatorisch (sehr kritische Zahlungen) und für welche sie fakultativ (kritische Zahlungen) ist. Mit Kasten 5 am Ende des Kapitels („Aspekte, die bei der Entscheidung über kritische Zahlungen zu berücksichtigen sind“) soll Krisenmanagern eine Entscheidungshilfe für die Abwicklung kritischer Zahlungen dargereicht werden.

Die Contingency-Abwicklung umfasst die manuelle Abwicklung von Zahlungen während eines Ausfalls der Gemeinschaftsplattform.

Ein SSP-Ausfall bedeutet, dass die Zahlungsmöglichkeiten der Banken in der Gemeinschaftsplattform blockiert wären. Aufgrund der nachstehenden Einschränkungen ist der Durchsatz im Contingency-Fall sehr begrenzt.

- Frische Liquidität muss bereitgestellt werden.
- Beschränkung der Kapazität des CM auf rund 1 000 Zahlungen pro Stunde.
- Es können keine Dateien aus Nebensystemen verarbeitet werden.

Das CM wird stets in der nicht aktivierten Region betrieben. Bestätigen die Settlement-Manager die Notwendigkeit der Abwicklung sehr kritischer Zahlungen, wird das CM sofort eingesetzt. Stehen keine sehr kritischen, sondern lediglich kritische Zahlungen zur Verarbeitung an, müssen die Krisenmanager zunächst bestätigen, dass diese über das CM abzuwickeln sind.

Der Valutatag des CM ist stets der, den die Gemeinschaftsplattform zum Zeitpunkt des Ausfalls hatte. Das CM bietet nur eine eingeschränkte Funktionalität und ist deshalb nicht mit einem „Mini-RTGS“ zu vergleichen (es gibt keine Algorithmen zur Zahlungsabwicklung, und spezielle Funktionen für die Abwicklung in Nebensystemen werden nicht unterstützt).

6.4.2.1 Aktivierungsverfahren für das Contingency-Modul

Der Beschluss, das CM für sehr kritische Zahlungen zu aktivieren und zu nutzen, wird von den Settlement-Managern in ihrer Telekonferenz gefasst. Bei Auslösung der Contingency-Abwicklung werden die Teilnehmer über sämtliche Kommunikationskanäle, die im vorliegenden Dokuments in Abschnitt 2.4.1 („Kommunikationsmittel”) und 5.3 („Kommunikation bei Störungen”) erläutert sind, informiert.

Das CM beginnt mit einem Saldo von null, d. h. die Zahlungskapazität der Gemeinschaftsplattform steht für eine Contingency-Abwicklung über das CM nicht zur Verfügung. Folglich erfordert die Abwicklung von Contingency-Zahlungen im CM die Bereitstellung frischer Liquidität durch die TARGET2-Nutzer.

Das CM wird ausschließlich von den Zentralbanken betrieben, und nur sie haben Zugriff. Die TARGET2-Nutzer übermitteln Aufträge zur Abwicklung von Contingency-Zahlungen an ihren jeweiligen „National Service Desk“ über die national vereinbarten Kommunikationsmittel und Abläufe. Angaben bezüglich Umsatz und Kontosalden im CM werden den TARGET2-Nutzern ebenfalls vom jeweiligen „National Service Desk“ über die vereinbarten nationalen Kommunikationswege zugeleitet.

Während die Abwicklung sehr kritischer Zahlungen obligatorisch ist, erfordert ein Antrag auf Verarbeitung kritischer Zahlungen die Einbeziehung der Krisenmanager mittels Telekonferenz.

Für die Dauer der Nutzung des CM erfolgen keine SWIFTNet FIN-Nachrichten an die Kontoinhaber im CM.

6.4.2.2 Zahlungsabwicklung im Contingency-Modul

1. TARGET2-Nutzer, die Contingency-Zahlungen vornehmen wollen, müssen dazu frische Liquidität bereitstellen.

Dies kann in Form von zusätzlichen Sicherheiten/Kontosalden oder über eingehende Zahlungen bzw. im CM erfolgende Zahlungen geschehen, durch die Liquidität im Euroraum (um)verteilt wird (z. B. Auszahlungen von Nebensystemen, Liquiditätsübertragungen zwischen Finanzinstituten, geldpolitische Geschäfte). Die Verfahren zur Bereitstellung zusätzlicher Sicherheiten hängen von den jeweiligen nationalen Vorkehrungen ab.

2. Sobald die NZB für einen TARGET2-Nutzer frische Liquidität im CM verbucht hat, kann die Contingency-Abwicklung für diesen Nutzer beginnen.

3. Der Sender weist seine Zentralbank an, über die jeweiligen nationalen Kommunikationsmittel und national vereinbarten Abläufe, Contingency-Zahlungen vorzunehmen. Sehr kritische Zahlungen können sofort verarbeitet werden, während für kritische Zahlungen zunächst ein Beschluss der Krisenmanager erforderlich ist.

4. Die sendende Zentralbank verbucht die Zahlung im CM (Belastung und Gutschrift erfolgen gleichzeitig).

5. Nach der Buchung informiert die sendende Zentralbank die Empfänger-Zentralbank. Nachdem Letztere die Buchung geprüft hat, informiert sie den Begünstigten mittels der national vereinbarten Kommunikationswege über den Zahlungseingang.

6.4.2.3 Weitere Einzelheiten zur Nutzung des Contingency-Moduls

- Auskünfte über Kontosalden, Belastungen und Gutschriften im CM können nur von den Zentralbanken eingeholt werden. TARGET2-Nutzer müssen daher diese Informationen bei ihrer Zentralbank anfordern, wobei die von der jeweiligen Zentralbank festgelegten Verfahren für Contingency-Situationen einzuhalten sind.
- Im CM sind nur Überweisungen möglich. Deshalb müssen alle CM-Transaktionen von der sendenden Bank veranlasst werden. Dies ist besonders für einige Nebensysteme von Bedeutung.
- Um die Anzahl der Contingency-Zahlungen zu verringern, sind die TARGET2-Nutzer aufgefordert, von Sammelüberweisungen Gebrauch zu machen.
- Hat ein TARGET2-Nutzer eine Zahlung an die Gemeinschaftsplattform übermittelt, die zunächst in die Warteschlange eingestellt wurde, und wickelt diese erneut über das CM ab, lässt sich eine „doppelte Ausführung“ der Zahlung (zunächst im CM und dann nach Neustart der Gemeinschaftsplattform ein zweites Mal im Zahlungsmodul) nicht vermeiden. Der Sender trägt die alleinige Verantwortung, geeignete Maßnahmen zur Vermeidung von Doppelausführungen zu ergreifen.
- Nach Wiederherstellung der Gemeinschaftsplattform wird die normale Zahlungsabwicklung dort fortgesetzt. Wenn alle Zentralbanken bestätigt haben, dass die Nutzung des CM abgeschlossen ist, wird dieses geschlossen. Die CM-Salden werden auf die RTGS-Konten im Zahlungsmodul übertragen (keine Übertragung der einzelnen zugrunde liegenden Zahlungen), und die Kontoinhaber werden nach Ende des Geschäftstags mit MT 940/950 über die Buchungen informiert (optional). Bei Schließung des CM weisen alle Konten im CM einen Saldo von null auf.
- Das CM kann erneut gestartet werden, falls am selben Tag eine weitere Störung der Gemeinschaftsplattform eintritt.
- Im Allgemeinen ist das genaue Verfahren zwischen den TARGET2-Nutzern und ihrer jeweiligen Zentralbank auf nationaler Ebene festgelegt.

Kasten 4: Das Konzept (sehr) kritischer TARGET2-Zahlungen

Wichtigste Grundsätze:

- Die TARGET2-Contingency-Abwicklung sollte sich auf Zahlungen beschränken, die verarbeitet werden müssen, um ein systemisches Risiko während des Tages zu vermeiden.
- Aufgrund der strikten, technisch und operativ bedingten Volumenbeschränkungen in TARGET2-Contingency-Situationen sollte die Gesamtzahl der Contingency-Zahlungen möglichst gering gehalten werden.

In erster Linie sollten ausgehende TARGET2-Zahlungen berücksichtigt werden. Ausgehende Zahlungen sind Zahlungen, die von anderen Systemen benötigt werden. Eingehende CM-Zahlungen (z. B. Auszahlungen von Nebensystemen, Liquiditätsübertragungen zwischen Finanzinstituten, geldpolitische Geschäfte) könnten unter bestimmten Umständen als kritische Zahlungen betrachtet werden, wenn sich belegen lässt, dass sie zur Deckung (sehr) kritischer ausgehender Zahlungen benötigt werden. In diesem Fall können die Krisenmanager der Verarbeitung zustimmen. In jedem Fall sollte die Anzahl dieser Zahlungen strikt beschränkt bleiben.

Die nachstehenden Zahlungsarten werden als sehr kritisch oder kritisch betrachtet und kommen daher für eine Contingency-Abwicklung infrage:

Sehr kritische Zahlungen müssen in Contingency-Situationen verarbeitet werden (Reihenfolge: CLS, FIFO).

- Zahlungen im Zusammenhang mit Ausgleichszahlungen von TARGET2 an CLS (Einzahlungen – „pay-ins“)
- Zahlungen im Zusammenhang mit Ausgleichszahlungen von TARGET2 an EURO1 für den Zahlungsausgleich zum Tagesabschluss („pay-ins“) und
- Zahlungen im Zusammenhang mit Margenzahlungen von TARGET2 an zentrale Kontrahenten („pay-ins“).

Kritische Zahlungen können in einer Contingency-Situation verarbeitet werden, müssen aber von den Krisenmanagern zuvor genehmigt werden.

- Verrechnungszahlungen an im „interfaced“-Modus arbeitende Wertpapierabwicklungssysteme zur Echtzeitabwicklung

- zusätzliche ausgehende Zahlungen, sofern zur Vermeidung eines systemischen Risikos erforderlich, und
- eingehende CM-Zahlungen, wenn sich belegen lässt, dass sie zur Deckung (sehr) kritischer ausgehender Zahlungen erforderlich sind.

Anzumerken ist, dass gemäß dieser Definition die Liquiditätstransfers auf die/von den Geldkonten als kritische Zahlungen gelten würden und somit für die Verarbeitung im Contingency-Modus infrage kämen. Aufgrund der funktionalen Ausgestaltung von T2S kann das CM allerdings nicht für Liquiditätsübertragungen auf Geldkonten verwendet werden. Dennoch können sich durch die Möglichkeit, die Selbstbesicherung und die existierenden DCA-Salden zu nutzen, die Auswirkungen auf T2S verringern

Kasten 5: Aspekte, die bei der Entscheidung über kritische Zahlungen zu berücksichtigen sind

Zusätzlich zu den drei wichtigsten Grundsätzen (Vermeidung eines systemischen Risikos, Beschränkung des Verarbeitungsvolumens und Konzentration auf ausgehende Zahlungen) könnten folgende Aspekte die Krisenmanager bei ihrer Entscheidungsfindung unterstützen:

- Die Umstände des Ausfalls, insbesondere sein Zeitpunkt: Neben Tagesbeginn und Tagesende sind auch die Abwicklungszeiten der Nebensysteme kritisch. Mögliche systemübergreifende Konsequenzen, die Ursache des Ausfalls und seine Dauer sowie die voraussichtlich für die Wiederherstellung benötigte Zeit sind ebenfalls wichtige Aspekte.
- Der Geschäftstag: Es könnte von Bedeutung sein, ob eine Störung am Ende der Mindestreserve-Erfüllungsperiode, an einem Feiertag oder an einem Tag auftritt, an dem mit besonders hohen Zahlungsvolumina gerechnet wird.
- Der von Banken, Nebensystemen oder anderen Geschäftsbereichen der Zentralbank (z. B. im Zusammenhang mit geldpolitischen Geschäften) geäußerte Bedarf.
- Die Liquiditätsbeschränkungen: Eine Contingency-Verarbeitung würde zusätzliche Sicherheiten erfordern. Je mehr Zahlungen in einer Contingency-Situation abgewickelt würden, umso mehr zusätzliche Sicherheiten müsste eine Bank also stellen; je nach dem Zeitpunkt, an dem der Contingency-Fall eintritt, könnte sich die Bereitstellung solcher Sicherheiten als schwierig erweisen.

- Das Prinzip der Priorisierung – sehr kritische Zahlungen sollten im Allgemeinen vor kritischen Zahlungen verarbeitet werden (solange die kritischen Zahlungen nicht zur Auflösung einer Anstauung sehr kritischer Zahlungen benötigt werden).
- Die Maßnahmen zur Störungsbehebung könnten den Bedarf an Contingency-Zahlungen verringern. Beispielsweise könnten große Nebensysteme ihre Abwicklung um den gleichen Zeitraum verlängern, um den sich der Annahmeschluss von TARGET2 verzögert. Zahlungen in der Warteschlange würden verarbeitet, sobald die Gemeinschaftsplattform wieder verfügbar ist. Als weiteres Beispiel könnten Nebensysteme eine Verrechnung versuchen, selbst wenn der Annahmeschluss in TARGET2 verschoben wird.
- Die Contingency-Mechanismen des Marktes: Mögliche alternative Contingency-Mechanismen von einzelnen Nebensystemen und Banken (z. B. Einzahlungen in einer anderen Währung) könnten die Notwendigkeit verringern, im Contingency-Fall kritische Zahlungen abzuwickeln.

6.4.3 Verlängerung des Annahmeschlusses

Die Entscheidung, bei einem Ausfall der Gemeinschaftsplattform die Schließung hinauszuschieben, d. h. die Tagverarbeitungsphase zu verlängern, wird stets von den TARGET2-Krisenmanagern getroffen. Die angekündigte neue Schlusszeit ist der neue Annahmeschluss für Interbankzahlungen. Dabei informiert das Eurosystem die Nutzer so frühzeitig wie möglich über die mögliche Dauer der Verlängerung. Solange dies nicht absehbar ist, insbesondere, wenn ein längerer Ausfall der Gemeinschaftsplattform vorliegt, werden in regelmäßigen Abständen aktualisierte Lageinformationen bereitgestellt. Durch eine Verlängerung der Tagverarbeitungsphase verschiebt sich auch der Annahmeschluss für Kundenzahlungen um den gleichen Zeitraum, wobei davon ausgegangen wird, dass die Verlängerung des Annahmeschlusses mindestens fünfzehn Minuten vor dem eigentlichen Annahmeschluss für Kundenzahlungen (d. h. spätestens um 16.45 Uhr) bewilligt wird. Es ist nicht möglich, nur den Annahmeschluss für Kundenzahlungen zu verschieben.

Abgesehen von den geschilderten Situationen im Zusammenhang mit einem Ausfall der Gemeinschaftsplattform, die zu einer Verlängerung des Annahmeschlusses führen könnten, kommt es möglicherweise zu Situationen, in denen die Schlusszeit verschoben wird, um eine Bankenkrise in den Griff zu bekommen.

Grundsätzlich sollten TARGET2 und T2S für die Euro-Abwicklung immer am gleichen Valutatag in Betrieb sein, d. h., insofern TARGET2 am Tag D noch für die Geldverrechnung in Euro geöffnet ist, sollte T2S keine Wertpapierverrechnung in Euro am Tag D+1 zulassen. Somit sollte im Falle einer verzögerten TARGET2-Schließung eine verzögerte T2S-Schließung, ein verzögerter T2S-Beginn des nächsten Abwicklungstags oder ein T2S-Start ohne die Möglichkeit der Verrechnung in Euro ins Auge gefasst werden. Ein Vorteil einer verzögerten T2S-Schließung könnte darin liegen, dass Sicherheiten über T2S aktiviert werden könnten, um Liquidität für eine Abwicklung im TARGET2-Contingency-Modul (CM) bereitzustellen.

Bei einer Verzögerung in TARGET2 informiert der TARGET2-Koordinator umgehend den T2S-Koordinator, damit der T2S-Prozess zur Störungsbehebung in Gang gesetzt werden kann. Doch wenn die Geldkonten über einen Null-Saldo verfügen, die Selbstbesicherungspositionen geschlossen sind und keine Wiederherstellungsaktivitäten nach dem Neustart im Anschluss an einen Katastrophenfall erforderlich sind, entfällt womöglich eine T2S-Verzögerung.

6.4.3.1 Verschiebung des Annahmeschlusses aufgrund eines zuvor aufgetretenen SSP-Ausfalls

Um dem Markt zusätzliche Betriebszeit zur Verfügung zu stellen, kann die Tagverarbeitungsphase verlängert werden, wenn ein Ausfall der Gemeinschaftsplattform im Laufe des Tages auftritt, aber vor 18.00 Uhr behoben wird. Eine solche Verlängerung sollte zwei Stunden nicht überschreiten und frühzeitig angekündigt werden, um den TARGET2-Nutzern Klarheit und Sicherheit zu verschaffen. Wird eine solche Verlängerung vor 16.45 Uhr gewährt, sollte zwischen den Annahmeschlusszeiten für Kunden- und für Interbankzahlungen weiterhin mindestens eine Stunde liegen. Eine Verlängerung der Annahmefrist könnte auch bewilligt werden, um die Bewältigung einer Bankenkrise zu erleichtern.

Sobald eine Verlängerung gewährt ist, darf sie nicht mehr zurückgenommen werden, selbst wenn dies technisch möglich wäre.

6.4.3.2 Verzögerter Annahmeschluss aufgrund einer anhaltenden SSP-Störung

Ein späterer Annahmeschluss wird bewilligt, wenn ein Ausfall der Gemeinschaftsplattform vor 18.00 Uhr auftritt und bis zu diesem Zeitpunkt nicht behoben ist. In solchen Situationen gibt es keine andere Möglichkeit, als die Wiederherstellung der Plattform abzuwarten.

Unmittelbar nachdem die TARGET2-Krisenmanager in ihrer Telekonferenz einen Aufschub des Annahmeschlusses genehmigt haben, werden die TARGET2-Nutzer über die einschlägigen nationalen Kommunikationswege, das ICM (falls verfügbar) und das T2IS darüber informiert. Die TARGET2-

Nutzer werden aufgefordert, ihre internen Vorgaben an die verzögerten Annahmeschlusszeit entsprechend anzupassen.

Bei einer Verlängerung der Annahmeschlusszeit sollten die TARGET2-Nutzer auch weiterhin SWIFTNet FIN-Nachrichten an die Gemeinschaftsplattform senden. Diese werden in eine Warteschlange gestellt und verarbeitet, sobald die Gemeinschaftsplattform wiederhergestellt ist. Dem liegt das Prinzip zugrunde, dass TARGET2 alle in einer Warteschlange befindlichen Zahlungen mit gleichtägiger Wertstellung abwickelt, um die Plattform restlos und endgültig schließen zu können.

Schritte nach der Wiederherstellung der Gemeinschaftsplattform

Nachstehend wird von einem Ausfall der Gemeinschaftsplattform in der Tagverarbeitung ausgegangen. Tritt der Ausfall zu einem späteren Zeitpunkt auf, beispielsweise zu Tagesbeginn, sind lediglich die übrigen Schritte relevant (als Kästen dargestellt).

Am Tag der Störung

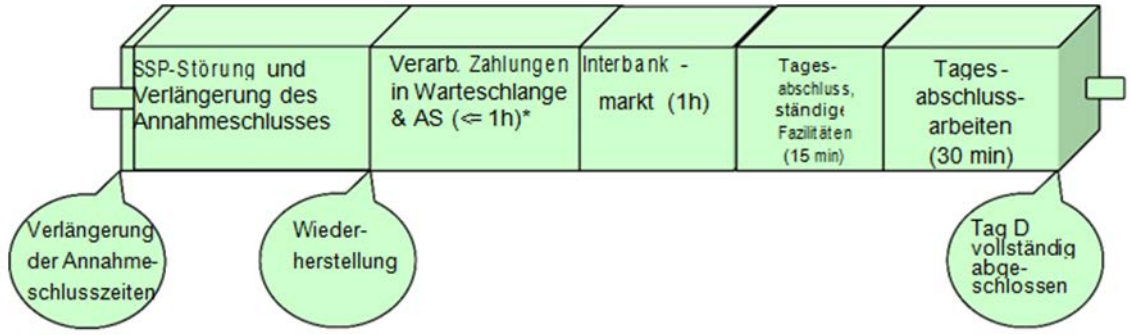

SSP-Störung und Verlängerung des Annahmeschlusses
Verarb. Zahlungen in Warteschlange & AS (<= 1h)*
Interbank - markt (1h)
Tages- abschluss, ständige Fazilitäten (15 min)
Tages- abschluss- arbeiten (30 min)
Verlängerung der Annahme- schlusszeiten
Wieder- herstellung
Tag D vollständig abge- schlossen

Abbildung 17: Abläufe am Tag der Störung

Die Wiederherstellung der Gemeinschaftsplattform bedeutet, dass wieder Nachrichten über sie verarbeitet werden können. Nach der Wiederherstellung werden – vorausgesetzt, der SSP-Ausfall trat während der Tagverarbeitungsphase auf – folgende Schritte eingeleitet:

- Abwicklung aller in der Warteschlange befindlichen Zahlungen (maximal eine Stunde); bei einem Plattform-Ausfall binnen 30 Minuten vor dem Annahmeschluss für Interbankzahlungen verkürzt sich dieser Zeitraum auf 30 Minuten. Die TARGET2-Nutzer können in dieser Phase auch neue Nachrichten senden.

- Ausgleich der Salden der Banken untereinander (eine Stunde); dieser Zeitraum verringert sich auf 30 Minuten, falls der Ausfall der Plattform innerhalb der 30 Minuten vor dem Annahmeschluss für Interbankzahlungen erfolgt.
- Nach dem Annahmeschluss für Interbankzahlungen findet die Tagesendeverarbeitung (45 Minuten bzw. am Ende der Erfüllungsperiode eine Stunde) statt, einschließlich der Inanspruchnahme der ständigen Fazilitäten.

Die Gesamtdauer dieser Schritte beträgt maximal 2 Stunden und 45 Minuten.

Schritte nach Verlängerung des Annahmeschlusses am Tag D

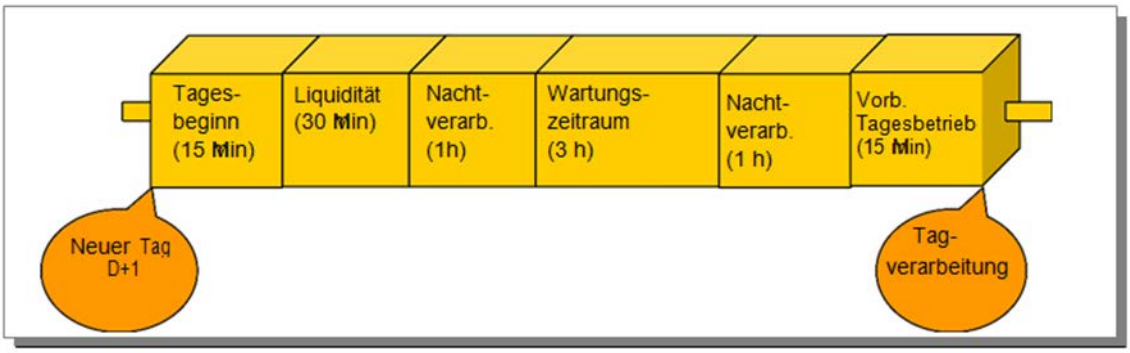


Abbildung 18: Ablauf am Tag nach der Störung

Außer den zuvor erwähnten obligatorischen Maßnahmen am Tag der Störung sind nach Abschluss des laufenden Geschäftstags mehrere obligatorische Schritte durchzuführen:

- Tagesbeginn (15 Minuten)
- Liquiditätsbereitstellung (30 Minuten)
- Nachtverarbeitung – NTS1 – einschließlich Liquiditätsbereitstellung an Geldkonten (mindestens 1 Stunde)
- Wartungsfenster (maximal 3 Stunden)
- Nachtverarbeitung - NTS2 (mindestens 1 Stunde)
- Vorbereitung der Tagverarbeitung (15 Minuten).

Diese Schritte summieren sich auf 6 Stunden und lassen sich weiter verkürzen durch die Reduzierung des Wartungsfensters und die Erleichterung der Nicht-Nachtverarbeitungsprozesse. Nachstehende Abbildung zeigt den Gesamtablauf:

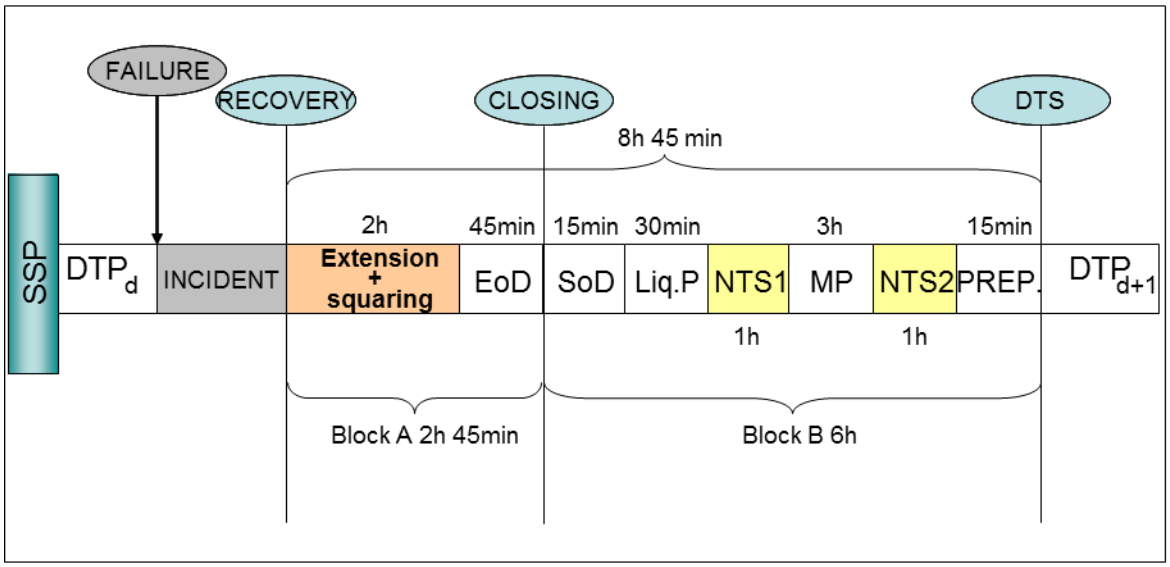


Abbildung 19: Überblick über die Abläufe im Fall einer Störung

Längerer Ausfall der Gemeinschaftsplattform

In Anbetracht der oben erwähnten Schritte wäre bei einem SSP-Ausfall während der Tagverarbeitungsphase und einer Wiederherstellung der Gemeinschaftsplattform bis 22.15 Uhr der Beginn der Tagverarbeitung um 7.00 Uhr noch möglich. Ein Ausfall, der sich über 22.15 Uhr hinauszieht (längerer Ausfall), könnte den Beginn der Tagverarbeitung um 7.00 Uhr verhindern, falls sich diese Phase (insbesondere das Wartungsfenster) nicht weiter verkürzen lässt.

Um Zeit einzusparen und die Tagverarbeitung möglichst bald nach 7.00 Uhr aufzunehmen, können die Schritte „Nachtverarbeitung 2“ und „Vorbereitung der Tagverarbeitung“ unmittelbar nach dem Wartungsfenster parallel erfolgen. Doch selbst durch dieses Vorgehen wäre ein Beginn der Tagverarbeitung um 7.00 Uhr womöglich noch nicht gesichert. Nebensysteme, die frühmorgens Liquidität in Euro benötigen, sollten für diesen Fall vorgesorgt haben.

6.5 Verfahren bei Störungen am Tagesende (18.00 Uhr - 18.45 Uhr)

Ein Ausfall der Gemeinschaftsplattform in dieser Phase würde die Tagesendeverarbeitung beeinträchtigen und somit möglicherweise auch die Inanspruchnahme der ständigen Fazilitäten, die Verfügbarkeit der endgültigen Kontosalden und den Beginn des neuen Geschäftstags. Die Ausführungen zur Verlängerung des Annahmeschlusses gelten hier in gleicher Weise wie oben beschrieben (siehe Abschnitt 6.4.3), wobei alle Annahmeschlusszeiten parallel zur ersten

Verlängerung verschoben werden. Der nächste Schritt nach der Wiederherstellung der Gemeinschaftsplattform wäre die Fortsetzung der Tagesendeverarbeitung.

7 Störungen auf der T2S-Ebene

7.1 Auswirkungen auf TARGET2

Je nach Zeitpunkt des Auftretens kann eine T2S-Störung die Liquidität der Payment Bank, die Bereitstellung von Sicherheiten und/oder die Rückerstattung von Innertageskrediten (einschließlich der Selbstbesicherung) beeinträchtigen, wie nachfolgend aufgezeigt wird. So ist es möglich, dass ein technisches Versagen von T2S den Banken über den gesamten Abwicklungstag Schwierigkeiten bei der Bereitstellung neuer Sicherheiten zur Erhöhung ihrer Kreditlinien verursacht.

Phasen eines Geschäftstags	Auswirkung einer T2S-Störung
Tagesbeginn 18.45 Uhr – 20.00 Uhr	Für 20.00 Uhr geplante Daueraufträge für Liquiditätstransfers könnte eine erneute Versendung erforderlich werden.
Nachtverarbeitung 20.00 Uhr – 03.00 Uhr	Die Liquidität der Geldkonten würde auf der T2S-Plattform verbleiben. Da keine Contingency-Abwicklung vorgesehen ist, um die Liquidität nach TARGET2 zurückzutransferieren, könnten (sehr) kritische Zahlungen, die (früh) in der TARGET2-Tagverarbeitung abzuwickeln sind (CLS, EURO1 Bridge, CCPs), beeinträchtigt werden.
Wartungsfenster 03.00 Uhr – 05.00 Uhr	Keine Auswirkungen auf TARGET2.
Echtzeitverarbeitung 05.00 Uhr – 18.00 Uhr	Eine verzögerte automatisierte Rückerstattung der Selbstbesicherung (16.30 Uhr) könnte zu Verzögerungen in TARGET2 – bis der Innertageskredit in T2S zurückerstattet werden kann – führen. Womöglich wäre die Frist für die Rückerstattung von Innertageskrediten durch angeschlossene Nicht-Eurosystem-NZBen zu verlängern. Liquidität könnte möglicherweise nicht wie geplant auf TARGET2 transferiert bzw. die geldpolitischen Geschäfte nicht auf TARGET2 weitergeleitet werden, was sich auf die Liquidität auswirken und einen Aufschub in TARGET2 erfordern könnte. Auswirkungen auf BATM mit Folgen für den Geldmarkt wären denkbar.
Tagesende 18.00 Uhr – 18.45 Uhr	Keine direkten Auswirkungen auf TARGET2.

Tabelle 11: Auswirkungen einer T2S-Störung auf TARGET2

Angesichts der in vorstehender Tabelle dargestellten Abhängigkeiten bei einer Störung der T2S-Plattform ist der T2S-Koordinator verpflichtet, den TARGET2-Koordinator so früh wie möglich zu informieren.

Grundsätzlich sollten TARGET2 und T2S für die Wertpapierverrechnung in Euro immer am gleichen Valutatag in Betrieb sein, d. h., insofern TARGET2 am Tag D noch für die Geldverrechnung in Euro geöffnet ist, sollte T2S für die Wertpapierverrechnung in Euro am Tag D+1 nicht öffnen und umgekehrt. Somit könnte im Falle einer verzögerten T2S-Schließung eine verzögerte TARGET2-Schließung oder ein verzögerter Beginn am nächsten Abwicklungstag ins Auge gefasst werden. Wenn allerdings die Geldkonten über einen Nullsaldo verfügen, die Selbstbesicherung zurückerstattet und keine Wiederherstellungsaktivitäten nach dem Neustart im Anschluss an einen Katastrophenfall erforderlich sind, könnte die Notwendigkeit einer verzögerten TARGET2-Schließung womöglich entfallen.

7.2 Situation einer T2S-Ausfallsicherung

Bei einer Störung der T2S-Plattform, die eine Ausfallsicherung auf einen anderen Standort oder eine andere Region auslöst, muss auf die Wiederherstellung der Plattform gewartet und gegebenenfalls die Schlusszeit bzw. die betreffende T2S-Phase verschoben werden (daher könnte je nach Tageszeit auch ein verzögerter TARGET2-Schluss erforderlich sein).

Die Zentralbanken sollten die Teilnehmer so früh wie möglich über die Lage informieren und empfehlen, dass keine neuen Nachrichten zur Belastung von/Gutschrift auf Geldkonten an die T2S-Plattform gesendet werden sollten (über die Direktverbindung zu T2S oder über die TARGET2-Kern- und/oder Zusatzleistungen für T2S). Regelmäßige Lageaktualisierungen erfolgen über die verfügbaren Kommunikationswege (wie in Abschnitt 2.4.1 beschrieben).

Bei einer interregionalen Ausfallsicherung (von Region 1 auf Region 2) werden die Zentralbanken, nachdem die T2S-Plattform in Region 2 wiederhergestellt ist, die Wiederherstellung und Synchronisierung der Euro-Zwischenkonten mit Blick auf die Salden und den Umsatz gewährleisten müssen – was aber lediglich im unwahrscheinlichen Falle eines Neustarts nach einem Katastrophenfall mit Datenverlust erforderlich ist. Dabei werden die fehlenden Liquiditätstransfers ermittelt und die Teilnehmer von der entsprechenden Zentralbank über die geplanten Maßnahmen und den betroffenen Liquiditätstransfer informiert.

Mit Blick auf die **Liquiditätsübertragungen von PM- auf Geldkonten** könnten die folgenden Maßnahmen ergriffen werden:

a) Wurden die Liquiditätstransfers auf die Gemeinschaftsplattform, aber noch nicht auf die T2S-Plattform gebucht (d. h., es wurde keine camt.025-Quittung von T2S empfangen) und haben die an T2S gesendeten Nachrichten noch den Status „provided" oder „acknowledged", wird der TARGET2 Coordination Desk (in der Funktion als T2S-Zwischenkontoinhaber) die Nachrichten über ICM (RTGS-Bildschirm > Zahlungen und Nachrichten (Payments and messages) > Nachricht wählen (Select messages) > Mögliche Nachrichten für erneutes Senden (Possible Messages for Repeat Sending)) erneut übermitteln.

b) Wurden die Liquiditätsübertragungen auf der Gemeinschaftsplattform und auch auf der T2S-Plattform gebucht (d. h., eine camt.025-Quittung wurde empfangen), ist der Geschäftsfall aus der SSP-Perspektive abgeschlossen, und somit können Nachrichten über ICM nicht erneut gesendet werden. Daher erfolgt technisch eine erneute Übersendung (d. h., die Nachrichten werden von der Middleware erneut gesendet). Bei einer hohen Anzahl von Liquiditätstransfers könnte die Entscheidung getroffen werden, alle in den letzten zehn Minuten vor der Störung verarbeiteten Liquiditätsübertragungen erneut zu senden (die Doppelinput-Kontrolle auf der T2S-Seite verhindert, dass in Region 2 zuvor bereits verarbeitete Liquiditätstransfers in T2S ein zweites Mal verarbeitet werden). In diesem Fall sollten Geldkontoinhaber, die den Nachrichtenerhalt mit Blick auf T2S-Gutschriften und/oder oder dem Erreichen einer Obergrenze abonniert haben, die Meldungen im Zusammenhang mit der zweiten Buchung (auf Region 2) nicht beachten.

Was die Liquiditätsübertragung von Geld- auf PM-Konten betrifft, so wird die für den begünstigten PM-Kontoinhaber zuständige Zentralbank das PM-Konto belasten und das Guthaben nach Autorisierung durch den Geldkontoinhaber dem T2S-Zwischenkonto gutschreiben. In diesem Falle sollten – wenn sich der DCA-Inhaber für Benachrichtigungen über Gutschriften und/oder Untergrenzen entschieden hat – die Meldungen im Zusammenhang mit dem ersten (in Region 1 vor dem Katastrophenfall erfolgten) Liquiditätstransfer ignoriert werden. Nach der Wiederherstellung könnte der Geldkontoinhaber die Liquiditätsübertragung an das PM-Konto erneut veranlassen.

8 Andere Ausfälle

Dieses Kapitel behandelt Störungen auf der Ebene der Zentralbanken, der Nebensysteme und der Bankenebene (einschließlich des Falls einer unkontrollierten Nachrichtenflut) sowie auf der SWIFT-Ebene. Während ein Ausfall der Gemeinschaftsplattform (SSP) alle Zentralbanken gleichermaßen betrifft und ein einheitliches Verfahren erforderlich macht, liegt die Vorgehensweise bei den in diesem Kapitel beschriebenen Ausfällen weitgehend in der Verantwortung der jeweiligen Zentralbank, des betroffenen Nebensystems oder der jeweiligen Bank.

Im Allgemeinen ist das genaue Verfahren, auf das sich die Nutzer und ihre jeweilige Zentralbank geeinigt haben, auf nationaler Ebene festgelegt.

8.1 Störungen auf der Zentralbankebene

In TARGET2 werden Zahlungen in der SSP und/oder der T2S-Plattform abgewickelt. Ein teilweiser oder kompletter Ausfall einer Zentralbank führt demnach nicht dazu, dass die gesamte Bankengemeinschaft eines Landes keinen Zugriff auf TARGET2 hat. Allerdings kommen jeder Zentralbank spezielle Aufgaben und Pflichten innerhalb von TARGET2 zu. Wenngleich die Auswirkungen eines Zentralbank-Ausfalls in TARGET2 beschränkt sein dürften, müssen für jede Störung adäquate Maßnahmen zur Verfügung stehen, damit das Kreditgewerbe ordnungsgemäß bedient und das Risiko vermieden werden kann, dass ein Zentralbankproblem anderweitig überspringt.

Grundsätzlich wird jedes Problem, das in einer Zentralbank/einem PHA besteht und sich auf die Gemeinschaftsplattform und/oder die T2S-Plattform oder auf die Bankengemeinschaft auswirken könnte, so zeitnah wie möglich innerhalb der Zentralbanken besprochen. Entsprechend den jeweiligen nationalen Bestimmungen und Verfahren kann ein National Service Desk die Banken direkt über Probleme auf nationaler Ebene informieren.

8.1.1 Ausfall einer Zentralbank

Grundsätzlich ist das Übergreifen eines Problems zu vermeiden, indem die Auswirkungen so gering wie möglich gehalten werden. Dies bedeutet, dass jede Zentralbank zunächst auf ihre eigenen Contingency-Maßnahmen zurückgreift. Sollte dies nicht möglich oder nicht effizient sein, kann die Zentralbank Hilfe vom SSP Service Desk in Anspruch nehmen.

Ansprechpartner für die TARGET2-Nutzer ist der jeweilige National Service Desk. Ist dieser nicht verfügbar, sollten die Nutzer nach den nationalen Kommunikationsverfahren für Krisenfälle verfahren.

Die Auswirkung einer Störung auf der Zentralbankebene hängt von der Phase des Geschäftstags ab, wie nachfolgend gezeigt wird

Phase des Geschäftstags	Auswirkung / Verfahren bei Störungen
Tagesbeginn 18.45 Uhr – 19.00 Uhr	Für alle Störungen, die in diesem Zeitraum auftreten könnten, hat die jeweilige Zentralbank angemessene Back-up-Maßnahmen vorbereitet.
Nachtverarbeitung 19.00 Uhr – 07.00 Uhr	Nach der Liquiditätsbereitstellung haben etwaige Probleme auf Zentralbankebene keinen Einfluss auf den SSP- oder T2S-Betrieb.
Betriebsfenster 06.45 Uhr – 07.00 Uhr	Das Eurosystem nutzt das Betriebsfenster zur Vorbereitung der Tagverarbeitung. Bei Störungen gelten die Verfahren zur Störungsbehebung während der Tagverarbeitung.
Tagverarbeitung 07.00 Uhr – 18.00 Uhr	Störungen während der Tagverarbeitung könnten sich auf die Aktualisierung von Kreditlinien/Repogeschäften und auf die Ausführung der zentralbankbezogenen Geschäfte (geldpolitische Transaktionen, Bareinlagen und Abhebungen etc.) auswirken. Für all diese Fälle hat die jeweilige Zentralbank angemessene Back-up-Maßnahmen vorbereitet.
Tagesabschluss 18.00 Uhr – 18.45 Uhr	Störungen während der Tagesendeverarbeitung wirken sich in der Regel nicht auf die Gemeinschaftsplattform, T2S oder auf die Bankengemeinschaft aus.

Tabelle 12: Auswirkungen eines Zentralbankausfalls

8.1.2 Ausfall eines proprietären Heimatkontos (PHA)

Neben den oben beschriebenen Problemen, die durch den Ausfall einer Zentralbank entstehen können, kann der Ausfall eines PHA zu folgenden Problemen führen:

1) Liquiditätsversorgung zu Beginn des Geschäftstags ist nicht möglich
2) Liquiditätsüberträge auf Innertagesbasis zwischen dem PHA und dem Zahlungsmodul (PM) sind nicht möglich
3) Mindestreservehaltung und die Inanspruchnahme der ständigen Fazilitäten sind nicht möglich
4) die Umbuchung von Sicherheiten (Relocation of collateral) könnte (falls die Zentralbank-Selbstbesicherung nicht rechtzeitig zurückerstattet wurde) nicht möglich sein.

Es wird darauf hingewiesen, dass auf PHA-Ebene festgestellte Probleme gänzlich der nationalen Verantwortung obliegen und von der jeweiligen Zentralbank einzeln behoben werden. Es ist äußerst

wichtig, dass die Zentralbank sämtliche Vorkehrungen und Maßnahmen trifft, um die Auswirkungen eines PHA-Problems auf die Zahlungsabwicklung in der SSP möglichst gering zu halten.

Die Auswirkung eines PHA-Ausfalls lässt sich wie folgt darstellen:

Phase des Geschäftstags	Auswirkung
Tagesbeginn und Liquiditätsbereitstellung (18.45 Uhr – 19.30 Uhr)	Zu Beginn des Geschäftstags auftretende Störungen verhindern die automatische Übertragung von Liquidität von einem PHA auf ein PM-Konto. Sind keine PHA-Daten verfügbar, ist die Ausführung von Transaktionen nicht möglich. Möglicherweise können Transaktionen (z. B. Daueraufträge) auf der Grundlage der Abschlusssalden der PM-Konten der betreffenden Teilnehmer abgewickelt werden oder wenn gegen Überlassung neuer Sicherheiten Liquidität auf dem PHA bereitgestellt wird. Besondere Aufmerksamkeit gilt jenen Nutzern, die an der Nachtverarbeitung teilnehmen. Für diese muss die Liquidität vor 19.30 Uhr übertragen werden. Anderenfalls können die Krisenmanager beschließen, die folgende Phase zu verschieben, d. h. den Beginn der Nachtverarbeitung zu verzögern. Daraus könnten sich Folgewirkungen für die Liquiditätsbereitstellung an die Geldkonten ergeben. Es liegt im Ermessen des National Service Desk, ob der nationalen Teilnehmergemeinschaft PHA-Probleme mitgeteilt werden. Im Falle von Auswirkungen auf TARGET2 werden Informationen auch über das T2IS und das ICM kommuniziert.
Nachtverarbeitung 19.30 Uhr – 07.00 Uhr	Nach der Liquiditätsbereitstellung an die PM-Konten haben etwaige Probleme auf Zentralbankebene keinen Einfluss auf den Betrieb der SSP.
Betriebsfenster 06.45 Uhr – 07.00 Uhr	Das Eurosystem nutzt das Betriebsfenster zur Vorbereitung der Tagverarbeitung. Bei Störungen gelten die Verfahren zur Störungsbehebung während der Tagverarbeitung.
Tagverarbeitung (07.00 Uhr – 18.00 Uhr)	Störungen während der Tagverarbeitung bedeuten, dass das PHA keine Transaktionen/Geschäfte ausführen kann. Daher sind z. B. die automatische Aktualisierung von Kreditlinien und Liquiditätsüberträge während des Tages zwischen dem PHA und dem Zahlungsmodul (PM) dann nicht möglich. Überdies könnten sich Auswirkungen auf die Umbuchung von Sicherheiten (Relocation of collateral) zeigen (falls die Zentralbank-Selbstbesicherung nicht rechtzeitig zurückerstattet wurde). PHA-Daten noch verfügbar: Sind trotz einer PHA-Störung die Daten noch verfügbar, kann die Zentralbank geeignete Maßnahmen ergreifen, um die betreffenden Transaktionen durchzuführen. PHA-Daten nicht verfügbar Sind keine PHA-Daten verfügbar, ist die Ausführung von Transaktionen nicht möglich. Verlängerung der Annahmeschlusszeiten [der Annahmefrist?] (delayed closing): Bei einem PHA-Ausfall gewähren die Krisenmanager keine Verlängerung des Annahmeschlusses für TARGET2.

Tagesabschluss (18.00 Uhr – 18.45 Uhr)	Am Tagesende auftretende PHA-Probleme können sich auf die Rückübertragung von Guthaben und die Liquiditätsüberträge zu Beginn des nächsten Geschäftstags auswirken. Den nationalen Zentralbanken stehen angemessene nationale Verfahren zur Verfügung, um auf solche Szenarien zu reagieren.

Tabelle 13: Auswirkungen eines PHA-Ausfalls

8.2 Betriebs- oder technische Störungen auf Teilnehmerebene[62]

Tritt beim Inhaber eines PM- oder Geldkontos ein Problem auf, infolge dessen er keine Zahlungen abwickeln und/oder keine Liquiditätstransfers auf/von Geldkonten in TARGET2[63] vornehmen kann, dann sollte er seine Zentralbank informieren und mit ihr in regelmäßigem Kontakt bleiben. Er sollte zudem versuchen, das Problem so weit wie möglich mit eigenen Mitteln zu beheben.

Hierzu kann der DCA-Inhaber folgende Möglichkeiten nutzen:

- Liquiditätstransfers von Geldkonten zu PM-Konten über die T2S-Schnittstelle, wenn sich der PM-Hauptkontoinhaber für die TARGET2-Zusatzleistungen entschieden hat
- GUI für Geldkontoinhaber, die normalerweise A2A-Funktionen verwenden.

Hierzu kann der PM-Kontoinhaber folgende Möglichkeiten nutzen:

- interne Contingency-Lösungen
- über den normalen ICM-Zugang die Funktionalität der Ersatzzahlungen, welche a) die Initiierung von Zahlungen auf das CLS-Konto, das EURO1-Sicherheitenkonto oder das EURO1-Deckungskonto ermöglichen (Contingency-Zahlungen) und b) die Initiierung von Zahlungen zur Umverteilung von Liquidität (Ersatzzahlungen zur Umverteilung von Liquidität[64])
- Liquiditätstransfers vom PM-Konto auf das Geldkonto über normalen ICM-Zugang (falls der PM-Kontoinhaber normalerweise die A2A-Funktionen nutzt)
- dieselben Funktionalitäten über eine Stand-alone-Verbindung, wenn die normale ICM-Verbindung nicht mehr verfügbar ist.

62 Finanzielle Ausfälle werden in den Abschnitten 3.6 und 3.7 behandelt.

63 Einschließlich eines Problems mit der SWIFT-Verbindung zur SSP und/oder mit der direkten Verbindung zur T2S-Plattform über einen der lizenzierten Mehrwertnetzwerkdienstleister.

64 Ersatzzahlungen zur Umverteilung von Liquidität dienen ausschließlich der Umverteilung von überschüssiger Liquidität. Sie sollen vermeiden, dass die Liquidität auf dem PM-Konto des Teilnehmers verbleiben muss, das von einem technischen Ausfall betroffen ist. Sie sind von den zugrunde liegenden kommerziellen Zahlungen vollständig getrennt. Daher können die Kreditinstitute, an die Überschussliquidität umverteilt wird, andere Parteien sein, als die Teilnehmer, für die die zugrunde liegenden Zahlungen bestimmt sind. Außerdem müssen die Institute, auf die überschüssige Liquidität umgelenkt wird, keine direkten TARGET2-Teilnehmer sein, sofern die Mittel über TARGET2 transferiert werden.

Sind die Mittel eines Teilnehmers erschöpft, oder können sie nicht effizient eingesetzt werden, kann der Teilnehmer auf den National Service Desk zurückgreifen, der in solchen Situationen eine begrenzte Anzahl von Zahlungen im Auftrag des entsprechenden Teilnehmers durchführen kann.

Die genauen Contingency-Kommunikationsverfahren sind bilateral zwischen dem Teilnehmer und seiner Zentralbank festgelegt.

Der National Service Desk benachrichtigt die anderen Zentralbanken über die technischen Probleme eines Teilnehmers, sofern sich diese auf die Abwicklung von Nebensystemen auswirken oder systemische Risiken, vor allem mit möglichen grenzüberschreitenden Auswirkungen, hervorrufen könnten. Die Information der Bankengemeinschaft wird zwischen allen Zentralbanken koordiniert.

Der Systemausfall eines einzelnen Teilnehmers sollte in keinem Fall zu einer Verschiebung des Annahmeschlusses führen.

Kasten 6: Contingency-Zahlungen

Ersatzzahlungen über das ICM (sowohl im U2A- als auch im A2A-Modus) dürfen nur für die Verarbeitung von Zahlungen auf das CLS-Konto, das EURO1-Sicherheitenkonto oder das EURO1-Deckungskonto (Contingency-Zahlungen) und für Zahlungen zur Umverteilung von Liquidität b) die Initiierung von Zahlungen zur Umverteilung von Liquidität (Ersatzzahlungen zur Umverteilung von Liquidität) verwendet werden.

Im Rahmen dieser Beschränkungen liegt die Durchführung von Ersatzzahlungen im freien Ermessen der Banken, die diese benötigen und die auch das volle Kreditrisiko tragen. Contingency-Zahlungen wie auch Ersatzzahlungen zur Umverteilung von Liquidität sind ihrem Wesen nach vollgültige Zahlungsaufträge. Dies bedeutet, dass diese oder eine ähnliche Zahlung nach Wiederaufnahme des Normalbetriebs nicht erneut gesendet werden müssen.

Wenn die Funktionalität der Ersatzzahlungen verwendet wird, sind folgende Aspekte zu berücksichtigen:

- Bevor ein PM-Teilnehmer die Funktion verwenden kann, muss er deren Aktivierung bei der zuständigen Zentralbank beantragen. Die Aktivierung erfolgt mit sofortiger Wirkung.
- Auf Anfrage eines PM-Teilnehmers, der die ICM-Funktionalität verwendet, kann die zuständige Zentralbank andere TARGET2-Nutzer über solche Zahlungen zur Liquiditätsumverteilung informieren.
- Hatte ein Teilnehmer technische Probleme und beabsichtigt, die verspäteten ursprünglichen Zahlungen am nächsten Geschäftstag mit dem Datum des Geschäftstags der technischen Störung (der ursprünglichen Valuta) zu senden, ist dies der zuständigen Zentralbank am Tag des technischen Systemausfalls, d. h. vor dem Tag, an dem die Einzelzahlungen übermittelt werden, mitzuteilen. Dieser Antrag auf Aufhebung der Valutaprüfung muss die zuständige Zentralbank mindestens 30 Minuten vor dem Annahmeschluss von TARGET2 erreichen. Die Zentralbank sorgt dafür, dass die Valutaprüfung für diesen Sender am folgenden Geschäftstag deaktiviert wird, sodass die ursprünglichen Einzelzahlungen mit der ursprünglichen Valuta verarbeitet werden können. Die Abwicklung in TARGET2 erfolgt immer an dem Geschäftstag, an dem die Zahlung übermittelt wird; weicht die Valuta hiervon ab, so müssen alle Zinsanpassungen außerhalb des TARGET2-Systems vorgenommen werden.
- Sofern die Aufhebung der Valutaprüfung noch einen weiteren Tag benötigt wird, muss dies am vorhergehenden Geschäftstag mindestens 30 Minuten vor Annahmeschluss beantragt werden.

- Sobald der beantragende Teilnehmer alle entsprechenden Transaktionen abgeschlossen hat, informiert er seine Zentralbank darüber, und diese aktiviert die Valutaprüfung wieder.
- Bei der Initiierung von Ersatzzahlungen ist nicht nur auf den Saldo des PM-Kontos zu achten, sondern auch auf mögliche Belastungen des PM-Kontos, die nicht vom betreffenden Teilnehmer veranlasst werden, wie z. B. Zahlungen zur Verrechnung von Nebensystemen.
- Empfänger von Ersatzzahlungen sollten beachten, dass der BIC des Senders solcher Zahlungen dem des PM entspricht (TRGTXEPMXXX) und dass der Zahlungspflichtige/Auftraggeber der Zahlung nur anhand des BIC in Feld 52 der FIN-Nachricht ermittelt werden kann.

Ersatzzahlungen zur Umverteilung von Liquidität sollten auf der Grundlage einer vorher getroffenen individuellen bilateralen Vereinbarung erfolgen. Dabei sind die in den Richtlinien der Europäischen Bankenvereinigung zum Liquiditätsmanagement (European Interbank Liquidity Management Guidelines) definierten Marktgepflogenheiten zu befolgen.

8.3 Ausfall eines Nebensystems

Tritt bei einem Nebensystem ein Problem auf, sollte es bis zur Behebung so weit wie möglich auf eigene Contingency-Maßnahmen zurückgreifen. Hauptziel sollte sein, alle Nachrichten an die SSP über die normalen Kanäle zu verarbeiten, d. h. über die Nebensystem-Schnittstelle (Ancillary System Interface - ASI) oder gegebenenfalls über die Standard-Zahlungsschnittstelle. Dabei müssen sowohl die Verwendung der Zahlungsschnittstelle als auch die von einer Zentralbank gebotene Unterstützung im Vorfeld zwischen dem Nebensystem und seiner Zentralbank abgesprochen und vereinbart werden.

- Das Nebensystem kann in eigenem Ermessen von alternativen Möglichkeiten wie Back-up-Standorten und Multi-Zugangsportalen zu Multi-Netzwerkpartnern Gebrauch machen. Ebenso ist die Nutzung der Standard-Zahlungsschnittstelle zur SSP möglich, um „reine“ („clean“) Zahlungen zu leisten.
- Bei Bedarf kann die jeweilige Zentralbank das Nebensystem unterstützen, z. B. indem sie XML-Dateien verarbeitet oder in dessen Auftrag „reine“ („clean“) Zahlungen leistet. Es hängt von der einzelnen Zentralbank ab, ob das „AS Contingency Tool“ für das Nebensystem angeboten wird oder nicht.
- In besonderen Ausnahmefällen, in denen ein Risiko für das gesamte Eurosystem besteht, kann die jeweilige Zentralbank des Nebensystems eine Verlängerung des Annahmeschlusses für TARGET2

beantragen, damit das Nebensystem mehr Zeit hat, die Störung zu beheben oder ihre Auswirkungen zu minimieren. Die Krisenmanager entscheiden, ob der Annahmeschluss verlängert wird.

Jede Zentralbank entscheidet selbst, welches Support-Level sie ihren Nebensystemen vor allem während der Nachtverarbeitung zur Verfügung stellen möchte. Solche Contingency-Vereinbarungen müssen stets im Vorfeld zwischen dem Nebensystem und seiner Zentralbank vereinbart werden. Treten während der Nachtverarbeitung Störungen auf, sollte das Nebensystem grundsätzlich seine Zentralbank informieren und mit ihr die Contingency-Maßnahmen und die nationalen Kommunikationsmittel abstimmen. Darüber hinaus hat das Nebensystem seine Verrechnungsteilnehmer separat über das geplante Abwicklungsverfahren zu informieren.

Ein Nebensystem sollte seinen „National Service Desk“ von Ausfällen in Kenntnis setzen. Nach eigenem Ermessen gibt der „National Service Desk“ das Problem an die Zentralbanken weiter, vor allem wenn grenzüberschreitende Auswirkungen möglich sind. Die Information der Bankengemeinschaft wird zwischen allen Zentralbanken koordiniert.

8.3.1 Nebensysteme, die die Nebensystem-Schnittstelle nutzen

Einzahlungen (von TARGET2 an das Nebensystem) könnten nach einer der folgenden Methoden abgewickelt werden:

- Die jeweilige Zentralbank sendet im Auftrag des Nebensystems mit dem „AS Contingency Tool“ eine XML-Datei an die SSP[65]
- das Nebensystem sendet einen MT204, sofern es die Zahlungsschnittstelle verwenden kann, d. h. wenn seine SWIFTNet-Verbindung unterbrochen ist, seine SWIFTNet FIN-Verbindung aber noch funktioniert, oder die betreffende Zentralbank sendet im Auftrag des Nebensystems einen MT204 (in diesem Fall müssen alle erforderlichen Genehmigungen erteilt worden sein)
- die Verrechnungsbank könnte gebeten werden, „reine“ („clean“) PM-Zahlungen zugunsten des Nebensystems zu leisten, oder
- die Zentralbank der Verrechnungsbank führt die Zahlungen („mandated payments“[66]) im Auftrag der Verrechnungsbank und auf Grundlage der vom Nebensystem gelieferten Informationen aus.

65 In diesem Fall können Ein- und Auszahlungen wie auch bei der normalen Abwicklung via ASI gemeinsam gesendet werden, sofern die Abwicklungsverfahren 3, 4, 5 oder 6 Anwendung finden.

66 „Mandated payments“ sind Zahlungen, die von einer nicht an der Transaktion beteiligten Stelle (im Regelfall einer NZB oder einem Nebensystem im Zusammenhang mit einer Nebensystemverrechnung) im Auftrag einer anderen Stelle initiiert werden. Beispielsweise sendet eine NZB eine Überweisung (mit einer bestimmten Nachrichtenstruktur) im Auftrag eines ausgefallenen direkten Teilnehmers (nur in Contingency-Situationen). „Mandated payments“ auf technische Konten sind nicht möglich.

Auszahlungen (vom Nebensystem an TARGET2) könnten nach einer der folgenden Methoden abgewickelt werden:

- Die jeweilige Zentralbank sendet im Auftrag des Nebensystems mit dem „AS Contingency Tool“ eine XML-Datei an die SSP oder
- das Nebensystem leistet „reine“ („clean“) Zahlungen mithilfe der Zahlungsschnittstelle.

Verarbeitet die Zentralbank keine XML-Dateien im Auftrag des Nebensystems unter Nutzung des „AS Contingency Tool“, kommt der Reihenfolge der Abwicklung bei den Abwicklungsverfahren 4 und 5 besondere Bedeutung zu.

- Abwicklungsverfahren 4: Die Zentralbank überprüft in Abstimmung mit dem Nebensystem, dass alle Einzahlungen vor Beginn der Auszahlungsphase abgewickelt sind. Können nicht alle Einzahlungen abgewickelt werden, erfolgt die Rückabwicklung, indem die Zentralbank eine Rückbuchung vom Nebensystem-Konto zum Bankkonto veranlasst (sofern die Einzahlung abgewickelt wurde) oder die Zahlung storniert (sofern sie noch aussteht).
- Abwicklungsverfahren 5: Dieses verläuft wie das Abwicklungsverfahren 4, nur werden hierbei keine Zahlungen rückabgewickelt, da die Abwicklung nach dem „Alles oder nichts“-Prinzip erfolgt ist.
- Für Nebensysteme mit einem Garantiekonto-Verfahren findet Abwicklungsverfahren 4 Anwendung, mit der Ausnahme, dass die Zentralbank bei Bedarf und in Abstimmung mit dem Nebensystem das Garantiekonto[67] belastet, statt eine Einzahlung vorzunehmen.

Bei Abwicklungsverfahren 6 ist die Überwachung der Verrechnungsphasen entscheidend:

- Die jeweilige Zentralbank kann im Auftrag des Nebensystems unter Nutzung des „AS Contingency Tool“ Abwicklungsverfahren und Zyklen anstoßen,

  die betreffende Zentralbank kann im Auftrag des Nebensystems mit dem „AS Contingency Tool“ oder direkt mittels des ICM (Funktion „stop procedure/cycle“) Abwicklungsverfahren und Zyklen beenden.

Simulation des Empfangs einer technischen „XML notification message“

Ein Problem bei der Zustellung oder Verarbeitung einer technischen „XML notification message“[68] kann zu einer Blockierung des laufenden und folgender Abwicklungsprozesse im Nebensystem

[67] Falls das Nebensystem die Garantien in Anspruch nimmt, sind besondere Verfahren erforderlich.

führen. Daher sollten die Nebensysteme unbedingt in der Lage sein, den Empfang solcher Nachrichten zu simulieren. Dies sollte (nach Prüfung im ICM) auf eigene Initiative des Nebensystems geschehen oder auf Basis einer auf sicherem Weg übermittelten Bestätigung des Abwicklungsergebnisses durch den „National Service Desk“ (die Einzelheiten sind bilateral zu vereinbaren). Das Nebensystem kann sich letztlich in Abstimmung mit dem „National Service Desk“ für die geeignetste Methode entscheiden, d. h. den Empfang simulieren oder den Nicht-Erhalt anderweitig lösen.

8.3 2 Nebensysteme, die die Zahlungsschnittstelle nutzen

Einzahlungen (von TARGET2 zum Nebensystem) werden zwar nach wie vor auf normalem Wege abgewickelt, doch die Zentralbank muss das Nebensystem unter Umständen über nationale Kommunikationswege von eingehenden Zahlungen in Kenntnis setzen.

Auszahlungen (vom Nebensystem zu TARGET2) werden nach einer der folgenden Methoden vom Nebensystem abgewickelt:

i) Das Nebensystem kann „reine“ („clean“) Zahlungen über die Zahlungsschnittstelle (sofern es noch Zugang dazu hat) oder mittels Ersatzzahlungen über das ICM leisten.

ii) Die Zentralbank sendet eine Zahlung („mandated payment“), die dem Nebensystem belastet und der Verrechnungsbank gutgeschrieben wird. Die Zentralbank muss das Nebensystem unter Umständen über nationale Kommunikationswege von den abgewickelten Zahlungen in Kenntnis setzen.

8.4 Technische Suspendierung

Eine technische Suspendierung schützt die Gemeinschaftsplattform und/oder die T2S-Plattform vorübergehend vor umfangreichen, unkontrollierten Nachrichteneingängen (z. B. „denial of service messages“, i. d. R. außerhalb des SWIFTNet FIN-Bereichs). In solchen Situationen muss sofort reagiert werden, um eine Störung des reibungslosen Funktionierens der SSP und/oder der T2S-Plattform zu vermeiden. Es handelt sich hierbei um eine rein technische Maßnahme, die dann zum Einsatz kommt, wenn eine Zentralbank, eine Bank oder ein Nebensystem eine so ungewöhnlich hohe Zahl von Nachrichten an die SSP und/oder die T2S-Plattform sendet, dass deren einwandfreier Betrieb möglicherweise gefährdet ist.

Stellt das Eurosystem solch eine außergewöhnlich hohe und umfangreiche Nachrichtenflut fest, die das reibungslose Funktionieren der Gemeinschaftsplattform und/oder der T2S-Plattform gefährdet, kann es den

[68] Zum Beispiel: ASTransferNotice, ASInitiationStatus, ReceiptAS(1), ReturnAccountAS.

Sender vorsichtshalber technisch suspendieren. Die Ursachen für das unbeabsichtigte Senden werden sofort im Gespräch mit dem Sender erörtert und sobald diese geklärt sind, hebt das Eurosystem die technische Suspendierung auf. Je nach Situation könnten die Krisenmanager vorsorglich eine Verlängerung der Annahmeschlusszeit erwägen.

8.5 Ausfall von SWIFT

Bei einem SWIFT-Ausfall wird ein alternatives Contingency-Netzwerk zur Bereitstellung eines Zahlungskanals verwendet. Das Contingency-Netzwerk bewirkt bei einem lokalen Ausfall oder einem Gesamtausfall von SWIFT eine deutliche Erhöhung der Ausfallsicherheit von TARGET2 sowie der Stabilität des Gesamtsystems. Auch ohne SWIFT-Zugang können Zentralbanken über das Contingency-Netzwerk im Auftrag ihrer Kunden (sehr) kritische Ersatzzahlungen und Zahlungen zur Umverteilung von Liquidität sowie Nebensystemdateien senden und Liquiditätstransfers zwischen PM-Konten und Geldkonten darüber durchführen. Darüber hinaus sind sie in der Lage, die Konten ihrer Teilnehmer über das Contingency-Netzwerk zu überwachen (einschließlich der Geldkonten, die an die Haupt-PM-Geldkontoinhaber angebunden sind, welche sich für die TARGET2-Zusatzleistungen für T2S entschieden haben). Das Contingency-Netzwerk ist jedoch kein vollständiger Ersatz für das SWIFT-Netzwerk, da es keine Verbindung zwischen den Nutzern und ihren NZBen bietet und sich auf vereinbarte nationale Kommunikationsmittel stützt.

Das tägliche Volumen der abwickelbaren Zahlungen beläuft sich auf rund 3 000, wobei 2 300 (sehr) kritische Zahlungen und 700 einzelne Nebensystemtransaktionen verarbeitet werden. Dabei wird zwischen sehr kritischen Zahlungen, die unbedingt abgewickelt werden müssen, und kritischen Zahlungen, vor deren Abwicklung die Zustimmung der Krisenmanager einzuholen ist, unterschieden. In Kapitel 6.4.2 „Contingency-Abwicklung unter Einsatz des Contingency-Moduls“ wird das Konzept (sehr) kritischer TARGET2-Zahlungen dargelegt.

Das Contingency-Netzwerk lässt sich für ein Land, für mehrere Länder oder für alle an TARGET2 angebundenen Länder aktivieren. Für einen einzigen Teilnehmer erfolgt keine Aktivierung des Contingency-Netzwerks.

Mit der Aktivierung des Contingency-Netzwerks wird für alle Teilnehmer, die über die betroffenen Zentralbanken angebunden sind, automatisch die Funktionalität der Ersatzzahlungen freigeschaltet.

8.5.1 Verarbeitung von Zahlungen

Die TARGET2-Nutzer informieren ihre Zentralbank über die im Contingency-Modus abzuwickelnden Zahlungen. Die Zahlungsaufträge werden nach Maßgabe der zuvor auf lokaler Ebene vereinbarten Contingency-Kommunikationsverfahren an den National Service Desk gesendet.

Der National Service Desk verarbeitet mithilfe seines über das Contingency-Netzwerk bestehenden Zugriffs auf die ICM-Ersatzbildschirme die Zahlungsaufträge nach dem Vier-Augen-Prinzip. Die Abwicklung der Ersatzzahlungen wird überwacht. Die auftraggebenden Parteien erhalten vom National Service Desk eine Rückmeldung entsprechend den lokalen Contingency-Kommunikationsverfahren.

Dabei ist Folgendes zu berücksichtigen:

- Teilnehmer mit Zugang zum SWIFT-Netzwerk und Teilnehmer mit internetbasiertem Zugang können weiterhin Zahlungen senden, müssen jedoch ihre Aktivitäten so weit wie möglich auf das Senden (sehr) kritischer Zahlungen beschränken, damit auf der Empfängerseite kein zusätzlicher Arbeitsaufwand entsteht.
- Da die Transaktionsreferenznummer für Zahlungen, die über die Ersatz-Funktionalität abgewickelt werden, vom System erzeugt wird, kann keine Kontrolle zur Vermeidung von Doppeleinreichungen, die sich unmittelbar nach Wiederherstellung der Verbindung zum SWIFT-Netzwerk ergeben können, erfolgen. Teilnehmer, die die Verarbeitung von Ersatzzahlungen beantragen, sollten ihre Zahlungen nach Ende des SWIFT-Ausfalls einer genauen Prüfung unterziehen.
- Für Zahlungen, die über das Contingency-Netzwerk abgewickelt werden, wird das allgemeine Format für Ersatzzahlungen verwendet. Die Zahlungen werden im SWIFT-Format MT202 über SWIFTNet FIN (ohne Y-Copy) an den Empfänger gesendet. In Feld 72 ist das Codewort /BUP/ einzutragen. Sender der Zahlung ist der gemeinsame BIC des PM, d. h. TRGTXEPMXXX. Wie für alle anderen Ersatzzahlungen erhält der Kunde nach Wiederherstellung der Verbindung zum SWIFT-Netzwerk eine Belastungsanzeige (MT 900), sofern er dies beantragt hat.
- Liquiditätstransfers von PM-Konten auf Geldkonten können über das Contingency-Netzwerk abgewickelt werden. Liquiditätstransfers von Geldkonten auf die Haupt-PM-Konten können nur verarbeitet werden, wenn sich der Inhaber des PM-Hauptkontos für die TARGET2-Zusatzleistungen für T2S entschieden hat.
- Es ist gewährleistet, dass die über das Contingency-Netzwerk übertragenen Nachrichten nicht zurückgewiesen werden.

8.5.2 Verarbeitung von Dateien aus Nebensystemen

Nebensysteme, die keinen Zugang zur SSP herstellen können, müssen die XML-Nachrichtendateien erzeugen und sie über die auf nationaler Ebene vereinbarten Contingency-Mechanismen (privates Netzwerk, E-Mail, Fax u. a.) an die jeweilige Zentralbank weiterleiten. Dateien für alle sechs in TARGET2 vorgesehenen AS-Abwicklungsverfahren werden auch vom Contingency-Netzwerk unterstützt. Dabei ist zu beachten, dass das Tagesvolumen der aus Nebensystemdateien verarbeiteten Zahlungen auf 700 Transaktionen begrenzt ist. Darüber hinaus ist die Größe jeder Datei auf maximal 1 MB limitiert. Dateien, die diese Größe überschreiten, werden zurückgewiesen.

Über das Contingency-Netzwerk erhält die Zentralbank Zugang zum ICM und lädt die Datei im Auftrag des Nebensystems hoch.

Folgende Spezifikationen sind in diesem Zusammenhang von Bedeutung:

- Bei den Modellen 4 und 5 ist sowohl die Bestätigung als auch die Ablehnung der Verwendung des Garantiekonto-Verfahrens möglich.
- Bei Modell 6 kann über den ICM-Bildschirm neben der Beendigung eines Nebensystemzyklus auch das Eröffnen eines Zyklus oder Verfahrens erfolgen.
- Doppelte Dateien, die über verschiedene Netzwerke gesendet wurden, werden von der Gemeinschaftsplattform erkannt und zurückgewiesen, sofern ihr Betreff identisch ist und sie von derselben initiierenden Partei stammen.
- Bei Dateien, die über das ICM hochgeladen wurden, wird keine Benachrichtigung (ASTransferNotice, ReturnAccount, MT 900/910) an den Nutzer gesendet. Die Zentralbank kann den Status der über das ICM gesendeten Dateien verifizieren und das betreffende Nebensystem informieren.

9. Test der Contingency- und Business-Continuity-Maßnahmen

9.1 Geltungsbereich

TARGET2 umfasst die Gemeinschaftsplattform (SSP), proprietäre Heimatkonten (PHAs) und andere Anwendungen der Zentralbanken sowie Nebensysteme (AS) und sonstige Einheiten, die eine Verbindung zur SSP und/oder der T2S-Plattform ermöglichen bzw. mit ihr arbeiten.

Die Zentralbanken unterliegen dem Geltungsbereich der vom EZB-Rat verabschiedeten „Information security policy for TARGET2“ und haben somit dafür zu sorgen, dass ihre Infrastrukturen sicher und zuverlässig funktionieren. Dazu gehört auch, dass sie für alle als kritisch eingestuften Geschäftsfunktionen über angemessene Maßnahmen für Notfallsituationen (Contingency) und Vorkehrungen zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity) verfügen, die in regelmäßigen Abständen getestet werden.

Ein SWIFT-Ausfall ist nicht Bestandteil der Tests, da der EZB-Rat das Restrisiko eines solchen Ausfalls als hinnehmbar einstuft.

9.2 Ziel der Tests

Die Contingency- und Business-Continuity-Maßnahmen sollen gewährleisten, dass Ausfälle von TARGET2-Komponenten - auf welcher Ebene auch immer - nicht zu einer Störung des Betriebs von TARGET2 insgesamt führen.

Jeder Nutzer sollte zunächst seine eigenen Back-up-Maßnahmen einleiten. Die Gemeinschaftsplattform sieht Contingency-Vorkehrungen vor, um kurze Unterbrechungen aufseiten eines Teilnehmers oder einer Zentralbank oder der SSP bei der Verarbeitung (sehr) kritischer Zahlungen zu überbrücken. Darüber hinaus können die Zentralbanken den Nutzern andere Vorkehrungen bieten wie etwa ein „AS Contingency Tool“ oder „mandated payments“.

9.3 Funktionen und Zuständigkeiten

Die obligatorischen und optionalen Tests der Contingency- und Business-Continuity-Maßnahmen für die Gemeinschaftsplattform und die Umgebungen der Zentralbanken werden in gemeinsamer Zuständigkeit der Ebene 2 organisiert und von der EZB koordiniert.

Die „National Service Desks“ führen obligatorische Tests mit ihren kritischen Teilnehmern sowie optionale Tests mit den kritischen und den nichtkritischen Teilnehmern durch. Hierzu gehören auch

die Erstellung eines Testzeitplans, praktische Hilfen bei der Durchführung der Tests und das Zusammenstellen von Testberichten.

Der „TARGET2 Coordination Desk“ beteiligt sich bei Bedarf auf zwischenstaatlicher Ebene an der Organisation.

9.4 Testumgebung

Damit die Tests effektiv sind, sollten sie entweder in der Produktionsumgebung oder, sofern dies aufgrund des zusätzlichen operationellen Risikos als nicht sinnvoll erachtet wird, in einer möglichst ähnlichen Testumgebung durchgeführt werden.

Bei Tests mit Nutzern gilt deren Testumgebung der SSP als der Produktionsumgebung so ähnlich wie möglich.

Wenn neue SSP-Releases getestet werden, kann es mitunter vorkommen, dass die Testumgebung nicht auf derselben Version beruht wie die Produktionsumgebung. Was die PHA-Umgebungen anbelangt, so muss jede Zentralbank, die ein proprietäres Heimatkonto anbietet, eine Testumgebung bereitstellen, die der Produktionsumgebung so ähnlich wie möglich ist.

9.5 Häufigkeit und Planung

Die Tests der Contingency-Vorkehrungen müssen von allen kritischen Teilnehmern mindestens einmal alle sechs Monate durchgeführt werden. Die Business-Continuity-Maßnahmen müssen von allen kritischen Teilnehmern mindestens einmal jährlich getestet werden, und es sollte nicht mehr als ein Jahr zwischen zwei Tests liegen.

Die Testumgebung der SSP ist standardmäßig an jedem Wochentag von 6.30 Uhr bis 19.00 Uhr (freitags bis 17:30 Uhr) geöffnet. Der Annahmeschluss für Interbankzahlungen liegt bei 15.30 Uhr.[69] Ausnahmen werden vorab mitgeteilt.

9.6 Testergebnisse und -berichte

Die Testergebnisse müssen als „erfolgreich“ oder „nicht erfolgreich“ klassifiziert werden. Werden die Testziele nicht erreicht, ist das Testergebnis als nicht erfolgreich anzusehen. Nicht erfolgreiche Tests sind innerhalb von drei Monaten zu wiederholen.

Nebensysteme und Banken melden die Testergebnisse gemäß den Anweisungen des National Service Desk.

[69] Seit 1. Juli 2014.

Die „National Service Desks“ liefern dem „TARGET2 Coordination Desk“ der EZB in regelmäßigen Abständen zusammenfassende Berichte und ermöglichen so eine systemweite Überwachung und Beurteilung, die dann in die jährliche Berichterstattung zu TARGET2 einfließt und gegebenenfalls Folgemaßnahmen nach sich zieht.

9.7 Test der Contingency-Maßnahmen

9.7.1 Kritische Teilnehmer

PM-Kontoinhaber können zwei verschiedene Arten von Ersatzzahlungen verwenden, um Zahlungen über das ICM zu veranlassen, wenn die normale Zahlungsabwicklung unterbrochen ist.

- Contingency-Zahlungen werden eingesetzt, um Einzahlungsverpflichtungen gegenüber CLS, dem EURO1-Sicherheitenkonto oder dem EURO1-Deckungskonto (TARGET2/EURO1-Liquiditätsbrücke) zu erfüllen. Die Contingency-Zahlung ersetzt die ursprüngliche Zahlung.
- Ersatzzahlungen zur Umverteilung von Liquidität erlauben es einem PM-Kontoinhaber, Liquidität, die sich auf seinem Konto angesammelt hat, umzulenken und einen etwaigen Aufbau von Überschussliquidität, welche die Effizienz von TARGET2 beeinträchtigen und möglicherweise zu systemischen Risiken führen könnte, zu vermeiden.

Kritische Teilnehmer, die die Funktion der Ersatzzahlungen oder ein zusätzliches Angebot ihrer Zentralbank (z. B. ein „AS Contingency Tool“ oder „mandated payments“) nutzen möchten, sollten nach zeitlicher Abstimmung mit der betreffenden Zentralbank mindestens zweimal pro Jahr eines der fünf nachstehenden Testszenarien durchlaufen:

1) Beantragung der Aktivierung der Backup-Funktion für Ersatzzahlungen im Live-Betrieb bei der Zentralbank und Senden der entsprechenden Ersatzzahlungen als Niedrigwertzahlungen (unter 10 €, verschiedene Beträge) auf vorher festgelegte Konten. Die Zentralbanken können ihre Konten als Empfänger der Zahlungen anbieten, wenn kein anderer Geschäftspartner für Testzwecke verfügbar ist.
2) Die Zentralbanken sollten in der Lage sein, die kritischen Zahlungen im Auftrag ihrer kritischen Teilnehmer unter Verwendung der Backup-Funktion auszuführen und dies gemeinsam mit ihnen zu testen.
3) Falls Tests in der Live-Umgebung als zu risikoträchtig eingeschätzt werden, kann dieselbe Art von Tests alternativ in der Testumgebung vorgenommen werden. Für die Betragshöhe gibt es dann keine Begrenzung.

4) Zentralbanken, die ihren Nebensystemen das „AS Contingency Tool“ anbieten, sollten dessen Funktionsfähigkeit testen.
5) Zentralbanken, die ihren kritischen Teilnehmern „mandated payments“ anbieten, sollten deren Funktionsfähigkeit testen.

Die Zentralbanken können nach Absprache mit ihren TARGET2-Nutzern beschließen, die Anzahl der Tage und die Zeiten für die Durchführung solcher Tests zu begrenzen, oder sie können diese Tests als ständiges Angebot bereithalten, das an jedem Tag, an dem die jeweilige Umgebung in Betrieb ist, in Anspruch genommen werden kann. Bei einer Begrenzung der Testzeit hat die Zentralbank darauf zu achten, dass jedem kritischen Teilnehmer genügend Gelegenheiten geboten werden, um die jeweiligen Tests mindestens alle drei Monate durchführen zu können.

Nicht kritische Teilnehmer sollten in regelmäßigen Abständen ähnliche Testübungen mit ihrem jeweiligen National Service Desk vorsehen.

9.7.2 Gemeinschaftsplattform (Testen der Contingency-Module)

Das Contingency-Modul (CM) ist das gemeinsame obligatorische Instrument zur Bewältigung von Notfallsituationen, wenn die normale PM-Funktionalität nicht gegeben ist, (sehr) kritische Zahlungen aber trotzdem abgewickelt werden müssen. Nur die Zentralbanken haben Zugriff auf das CM und können Zahlungen im Auftrag ihrer Nutzer ausführen. Diesbezüglich sollten alle Nutzer und Zentralbanken aktuelle Informationen über die Höchstzahl der pro Stunde abzuwickelnden (sehr) kritischen Zahlungen sowie über die in einer Notfallsituation für die Weiterleitung dieser Zahlungen jeweils verwendbaren Kanäle ermitteln und bereithalten. Dabei sollten die Zentralbanken ihre eigenen Verarbeitungserfordernisse sowie den Bedarf des Nutzers mit der höchstmöglichen Anzahl solcher Zahlungen pro Stunde berücksichtigen.

Wenngleich nur Zentralbanken direkt auf das CM zugreifen können, werden auch alle an der Abwicklung (sehr) kritischer Zahlungen beteiligten Nutzer in diesen Test mit einbezogen. Das Szenario besteht darin, dass die Nutzer die maximalen (sehr) kritischen Zahlungen pro Stunde an die Zentralbanken liefern und diese die entsprechende Verarbeitung im CM vornimmt. Die Nutzer sollten die maximale Anzahl der kritischen Zahlungen pro Stunde variieren. Die Zentralbanken bestätigen die abgewickelten Zahlungen über einen sicheren Kanal.

Die Nutzer suchen sich Geschäftspartner, mit denen sie Zahlungen austauschen können. Wenn Zahlungen zwischen verschiedenen Mitgliedstaaten Teil des Szenarios sind und der Geschäftspartner für Testzwecke nicht verfügbar ist, ersetzt die entsprechende Zentralbank den ausländischen Geschäftspartner mit einem ihrer eigenen Konten.

Damit die Tests so effektiv wie nur möglich sind und einer echten Notfallsituation nahekommen, umfasst der Test zwischen den Zentralbanken und ihren Nutzern auch die Bereitstellung frischer Liquidität im CM.

Der „SSP Service Desk“ testet dasselbe Szenario, indem er im Auftrag der Zentralbank agiert, die das höchste von allen Zentralbanken vorgesehene Volumen pro Stunde an (sehr) kritischen Zahlungen ausführt.

Zu Testzwecken aktiviert der SSP Service Desk mittwochs zwischen 10.00 Uhr und 12.00 Uhr das CM in der Testumgebung. Tests außerhalb dieses Zeitrahmens müssen über den zuständigen National Service Desk beim SSP Service Desk beantragt werden.

Darüber hinaus organisiert die EZB alle sechs Monate Testläufe für das CM unter Produktionsbedingungen. Jeder Testlauf umfasst eine Gruppe von Zentralbanken. Die Zentralbanken können beschließen, auch TARGET2-Nutzer mit einzubinden. An diesen Tagen aktiviert der SSP Service Desk das CM parallel zum Normalbetrieb in der Produktionsumgebung. Auf diese Weise lässt sich verifizieren, dass sowohl die Anbindung an das CM als auch eine angemessene technische Anordnung der TARGET2-Nutzer für den Live-Betrieb des CM gegeben sind. Volumentests werden nicht durchgeführt.

9.8 Test der Business-Continuity-Maßnahmen

9.8.1 Kritische Teilnehmer

Jeder Nutzer, der vom Eurosystem im Hinblick auf das reibungslose Funktionieren von TARGET2 als kritisch eingestuft wurde, muss über eine Strategie zur Aufrechterhaltung des Geschäftsbetriebs verfügen, die folgende Elemente aufweist:

- Business-Continuity-Pläne wurden erstellt, und Verfahren zu deren Einhaltung sind vorhanden.
- Es muss ein Ausweichstandort vorhanden sein.
- Das Risikoprofil des Ausweichstandorts muss sich von dem des Primärstandorts unterscheiden (deutliche Entfernung zwischen den Standorten, anderes Energieversorgungsnetz, andere Hauptfernmeldeleitungen usw.).
- Im Falle einer größeren Betriebsstörung, die dazu führt, dass auf den Primärstandort nicht zugegriffen werden kann und/oder für den Betrieb notwendige Mitarbeiter nicht verfügbar sind, muss der kritische Teilnehmer in der Lage sein, den normalen Betrieb vom Ausweichstandort aus

wiederaufzunehmen; dabei muss es möglich sein, vom Ausweichstandort aus den Geschäftstag ordnungsgemäß abzuschließen und den/die folgenden Geschäftstag(e) zu beginnen.

- Es müssen Verfahren etabliert sein, die gewährleisten, dass die kritischsten Transaktionen während der Verlagerung vom Primärstandort auf den Ausweichstandort ausgeführt werden können.
- Die Fähigkeit, Betriebsstörungen zu bewältigen, wird mindestens einmal jährlich geprüft, und alle wichtigen Mitarbeiter werden angemessen geschult. Der Abstand zwischen den Tests sollte nicht länger als ein Jahr sein.

Unter Berücksichtigung der vorstehend genannten Punkte lassen sich die Business-Continuity-Testanforderungen folgendermaßen zusammenfassen:

- Mindestens einmal im Jahr müssen die kritischen Teilnehmer ihre Business-Continuity-Verfahren testen, vom Sekundärstandort aus ihre kritischen Transaktionen ausführen und von dort den Geschäftstag abschließen (siehe Abschnitt 9.4 „Testumgebung").
- Die kritischen Teilnehmer müssen den jeweiligen National Service Desk vorab vom Business-Continuity-Test in Kenntnis setzen und ihn im Anschluss über die Testergebnisse informieren.

9.8.2 SSP

Die Business-Continuity-Maßnahmen umfassen die bestehenden Verfahren und Infrastrukturen für die Gemeinschaftsplattform, die bei einem Ausfall oder einer Notfallsituation eine Ausfallsicherung zum Ersatzstandort innerhalb derselben oder in einer anderen Region ermöglichen. NZBen, die ein PHA unterhalten, sowie kritische Teilnehmer sollten ähnliche Verfahren und Infrastrukturen besitzen. Darüber hinaus sind die Überwachungsanforderungen zur Gewährleistung der Business Continuity bei systemrelevanten Zahlungssystemen zu beachten.

Die folgenden Szenarien sind in regelmäßigen Abständen zu testen, d. h. intraregionale Ausfallsicherung und interregionale Ausfallsicherung. Derartige Tests werden an Wochenenden standardmäßig in der Produktionsumgebung durchgeführt, wobei die Nutzer nicht zwangsläufig einbezogen werden müssen. Sie können über den National Service Desk gebeten werden, an den Tests teilzunehmen. In Ausnahmefällen können ähnliche Tests in der Testumgebung durchgeführt werden.

10. Change- und Release-Management-Verfahren

In diesem Kapitel werden das jährliche Release-Management-Verfahren sowie das Änderungsverfahren bei Notfalländerungen und „Hot Fixes“ mit Blick auf die SSP beschrieben. Veränderungen der geldbezogenen Funktionalitäten auf der T2S-Plattform sollten im Einklang mit dem Change- und Release-Management-Verfahren erfolgen, das in der T2S-Rahmenvereinbarung – Schedule 9 beschrieben wird.

10.1 Jährliches Release

Das Eurosystem ist bestrebt, das TARGET-System stets an die verschiedenen Geschäftsänderungen auf dem Gebiet der Großbetragszahlungen anzupassen. Dieses kontinuierliche Interesse an einer Weiterentwicklung des Systems wird als notwendig erachtet, um das Niveau der angebotenen Dienstleistungen und die Zufriedenheit der Nutzer weiter zu erhöhen. Daher ist es äußerst wichtig, dass alle TARGET2-Nutzer in angemessener Form und zeitnah in den Prozess des Release Managements eingebunden werden.

TARGET2-Releases erscheinen im Allgemeinen jährlich, und zwar zeitgleich mit dem jährlichen SWIFT Standard Release im November. In Ausnahmefällen kann jedoch auch in einem Jahr ein zusätzliches (d. h. zweites) oder gar kein Release herausgegeben werden.

Das jährliche TARGET2-Release durchläuft ein langes, 21 Monate dauerndes Verfahren, damit alle Parteien genügend Zeit zur Erörterung, Priorisierung, Umsetzung und zum Testen haben. Außerdem werden den TARGET2-Nutzern alle Informationen so früh zur Verfügung gestellt, dass sie die Änderungen gut planen und budgetieren können.

10.1.1 Wichtige Termine

Alle in diesem Abschnitt genannten Termine sind unverbindlich und werden vom Eurosystem für jedes jährliche Release im Laufe des Februar des Jahres J-1 bestätigt. Das Eurosystem ist zwar bestrebt, die Termine weitestgehend einzuhalten, doch sind bei Bedarf und nach Absprache mit den Nutzern geringfügige Abweichungen möglich.

Jahr J-1	Mitte Februar	Bestätigung der endgültigen Termine
	Anfang März – Mitte April	Erste Konsultation der Nutzer
	Mitte September – Mitte Oktober	Zweite Konsultation der Nutzer
	Mitte November	Bekanntgabe des Release-Inhalts

Jahr J	Anfang März	Lieferung der UDFS
	Mitte April	Lieferung der Testpläne und -szenarien
	Ende August	Testbeginn durch die Nutzer
	Mitte November	Inbetriebnahme

Tabelle 14: Zeitplan für das jährliche Release

10.1.2 Einbindung der Nutzer

Im Rahmen der Erörterungen zum Inhalt des jährlichen TARGET2-Release werden zwei Konsultationsverfahren mit der Nutzergemeinschaft durchgeführt. Um alle TARGET2-Nutzer in die Ausarbeitung des Release-Inhalts einzubeziehen, setzen sich die nationalen Zentralbanken der an TARGET2 angeschlossenen Länder mit ihren jeweiligen nationalen Nutzergruppen in Verbindung. Gleichzeitig tritt die EZB an die TARGET Working Group (TWG) der europäischen Bankenverbände (European credit sector associations – ECSAs) heran.[70]

- Im ersten Konsultationsverfahren werden Vorschläge aller Nutzer für funktionale Änderungen zusammengetragen. Diese Vorschläge sollen hinreichend detailliert sein und einer großen Zahl von Nutzern zugutekommen. Zur Vereinfachung der Konsultation werden als Diskussionsgrundlage eine Liste funktionaler Änderungen, die im Zuge früherer Releases vorgeschlagen wurden, sowie von Zentralbanken unverbindlich angeregte Modifikationen vorgelegt, die jeweils mit eindeutigen Referenznummern gekennzeichnet sind. In jedem Vorschlag sollten der jeweilige Geschäftsvorfall und die erwarteten funktionalen Änderungen präzise dargelegt werden. Das Eurosystem stellt für die Einreichung ein entsprechendes Formular zur Verfügung. Am Ende des ersten Konsultationsverfahrens prüft das Eurosystem sorgsam sämtliche Vorschläge der nationalen Nutzergruppen und der TWG und nimmt einen Teil der vorgeschlagenen Änderungen in die engere Wahl; für diese wird eine weitere Kosten-Nutzen-Analyse durchgeführt.
- Im zweiten Konsultationsverfahren werden die Rückmeldungen der Nutzer zu den aus der ersten Konsultation hervorgegangenen und von den Zentralbanken in die engere Wahl genommenen Änderungen erfasst. In diesem Stadium sind keine weiteren Änderungsvorschläge mehr möglich. Gegebenenfalls werden auch Angaben zu den Kosten der vorgesehenen Maßnahmen gemacht. Die Rückmeldungen müssen auf der Grundlage zuvor festgelegter Standardbewertungskriterien erfolgen. Am Ende der zweiten Konsultation prüft das Eurosystem alle Rückmeldungen der Nutzer

[70] Die europäischen Bankenverbände (European Credit Sector Associations - ECSAs) umfassen drei gesamteuropäische repräsentative Branchenverbände: die Europäische Bankenvereinigung (European Banking Federation - EBF), die Europäische Sparkassenvereinigung (European Savings Bank Group – ESBG) und die Europäische Vereinigung der Genossenschaftsbanken (European Association of Co-operative Banks - EACB).

und kommt zu einer abschließenden Einschätzung in Bezug auf den Inhalt des jährlichen TARGET2-Release. Dieser wird wenig später bekannt gegeben.[71]

Um den Nutzern die Darlegung ihrer Änderungswünsche zu erleichtern, wurde ein Formular für Änderungsvorschläge (Anhang IV) entworfen. Alle von den Nutzern vorgebrachten Änderungswünsche sind auf diesem Formular einzureichen. Jedes andere Formular wird abgewiesen und zurückgereicht.

10.1.3 Priorisierung und Entscheidungsfindung

Bei der Priorisierung der verschiedenen Vorschläge der Nutzer oder der endgültigen Entscheidung zum Release-Inhalt tragen die Zentralbanken folgenden Kriterien gebührend Rechnung:

- Für jede einzelne Änderung wird eine eingehende Kosten-Nutzen-Analyse durchgeführt. Dabei werden vor allem folgende Punkte in Betracht gezogen: die Rückmeldungen der Nutzergemeinschaft im Zuge der Konsultationsrunden, die durch die Änderung realisierte Verbesserung des Dienstleistungsangebots für den Bankensektor insgesamt, die erwartete Nutzung des neuen Merkmals, die damit verbundenen Investitionen und Betriebskosten, die Nachhaltigkeit der neuen Dienstleistung im Hinblick auf die Kostendeckung, die Komplexität der Entwicklungen sowie das mögliche Risiko, Regressionsfehler in das System einzubringen. Wann immer dies erforderlich ist, prüfen die Zentralbanken schließlich auch, inwieweit die Änderung mit der Politik oder Strategie des Eurosystems zu TARGET2 im Einklang steht.
- Die Zentralbanken sind bestrebt sicherzustellen, dass der Release-Inhalt insgesamt im Hinblick auf die Vorteile, die den verschiedenen Gruppen von Nutzern entstehen, ausgewogen ist und die für das jährliche Release festgelegten Höchstbelastungen für den Arbeitsaufwand und das Budget eingehalten werden.

Aus Transparenzgründen werden die Nutzer nach jedem Konsultationsschritt darüber informiert, warum eine Änderung ausgewählt oder verworfen wurde.

10.2 Notfalländerungen und Hot Fixes

In diesem Abschnitt sollen diejenigen Elemente des Change- und Release-Management-Verfahrens für die Gemeinschaftsplattform beschrieben werden, die eng mit dem täglichen TARGET2-Betrieb

[71] Das Eurosystem kann über Änderungen, die mit SWIFT zusammenhängen, zu einem späteren Zeitpunkt informieren, wenn der endgültige Inhalt des SWIFT FIN und CAMT Standard Release bekannt ist. Wenn durch das Release auch Fehler behoben werden, so werden diese Änderungen ebenfalls später bekannt gegeben.

zusammenhängen und als solche nicht Bestandteil des alljährlichen Release-Management-Verfahrens sind.

Folgende Arten von Änderungen können in der Zeit zwischen den jährlichen Standard-Releases zu einer Modifikation der Gemeinschaftsplattform führen:

1) Notfalländerungen
2) Kleinere Änderungen, die so schwerwiegend sind, dass sie als Hot Fix umgesetzt werden.

Alle weiteren Änderungen werden im Rahmen des normalen Change- und Release-Management-Verfahrens bei den jährlichen Releases berücksichtigt.

10.2.1 Notfalländerungen

Notfalländerungen kommen bei Systemfehlern zum Tragen, die einer sofortigen Änderung bedürfen, damit der Betrieb der SSP aufrechterhalten oder eine erhebliche Einschränkung der Service-Qualität verhindert wird. Solche Änderungen sind eng mit dem in Kapitel 5 („Grundlegende Aspekte der Verfahren für Ausnahmesituationen“) beschriebenen Verfahren zur Störungsbehebung verknüpft und können innerhalb eines TARGET2-Geschäftstages installiert werden. Beeinträchtigt eine Notfalländerung die von TARGET2-Nutzern verwendeten Funktionalitäten, so werden die Nutzer im Wege einer ICM-Nachricht darüber informiert.

10.2.2 Hot Fixes

Hot Fixes sind nur dann gerechtfertigt, wenn durch die ausbleibende Beseitigung eines Problems vor dem nächsten regulären Release erhebliche operationelle Probleme entstehen könnten, komplizierte Provisorien erforderlich wären und/oder es anderweitig zu einer deutlichen Zunahme der operationellen Risiken käme. Hot Fixes werden immer zuerst in der Testumgebung installiert und dort – soweit möglich – getestet. Falls dies aufgrund der Auswirkungen auf die Nutzer notwendig ist, werden alle Nutzer über eine ICM-Nachricht von dem bevorstehenden Hot Fix in Kenntnis gesetzt.

11. TARGET2-Ausgleichsregelung

11.1 Allgemeines

Wenn in TARGET2 eine technische Störung auftritt, können die Teilnehmer gemäß der TARGET2-Ausgleichsregelung in Anhang II der Harmonisierten Bedingungen für die Eröffnung und Führung eines PM-Kontos sowie in Anhang II der Harmonisierten Bedingungen für die Eröffnung und Führung eines Geldkontos (DCA-Kontos) Ausgleichsforderungen geltend machen.

Vorbehaltlich einer anders lautenden Entscheidung des EZB-Rates findet die TARGET2-Ausgleichsregelung keine Anwendung, wenn die technische Störung von TARGET2 durch äußere Ereignisse verursacht wurde, die außerhalb der Einflussnahmemöglichkeit der betreffenden Zentralbanken liegen, oder das Ergebnis von Handlungen oder Unterlassungen Dritter ist.

Ausgleichszahlungen gemäß der TARGET2-Ausgleichsregelung stellen den einzigen Ausgleichsmechanismus dar, der im Falle einer technischen Störung von TARGET2 angeboten wird. Die TARGET2-Teilnehmer können jedoch auf anderem rechtlichen Wege Ausgleichsforderungen geltend machen. Mit der Annahme eines Ausgleichsangebots im Rahmen der TARGET2-Ausgleichsregelung verzichtet der TARGET2-Teilnehmer unwiderruflich auf alle Ansprüche hinsichtlich der Zahlungsaufträge, für die er das Ausgleichsangebot angenommen hat (einschließlich aller Ansprüche auf Ausgleich für Folgeschäden), gegenüber jeder Zentralbank. Mit Erhalt der entsprechenden Ausgleichszahlung sind alle diese Ansprüche vollständig und endgültig abgegolten. Der Teilnehmer stellt die betreffenden Zentralbanken bis in Höhe des Betrags frei, den er im Rahmen der TARGET2-Ausgleichsregelung erhalten hat, und zwar hinsichtlich aller sonstigen Ausgleichsforderungen, die ein anderer Teilnehmer oder Dritter für den betreffenden Zahlungsauftrag oder die betreffende Zahlung geltend macht.

Ein Ausgleichsangebot stellt kein Haftungseingeständnis der betreffenden Zentralbank oder einer anderen Zentralbank in Bezug auf eine technische Störung von TARGET2 dar.

Nähere Informationen finden sich in Anhang II der Harmonisierten Bedingungen für die Eröffnung und Führung eines PM-Kontos sowie in Anhang II der Harmonisierten Bedingungen für die Eröffnung und Führung eines Geldkontos.

11.2 Verfahrensregeln

- Ausgleichsforderungen sind mit dem Antragsformular geltend zu machen, das auf der Website der betreffenden Zentralbank in englischer Sprache zur Verfügung steht. Zahler müssen für jeden

Zahlungsempfänger, Zahlungsempfänger für jeden Zahler ein gesondertes Antragsformular einreichen. Die Angaben im Antrag sind durch ausreichende Informationen und Unterlagen zu belegen. Je Zahlung oder Zahlungsauftrag darf nur ein Antrag eingereicht werden.

- Teilnehmer müssen ihre Anträge innerhalb von vier Wochen nach einer technischen Störung von TARGET2 bei der zuständigen Zentralbank einreichen. Weitere Informationen oder Belege, die die betreffende Zentralbank anfordert, sind innerhalb einer Frist von zwei Wochen nach Anforderung einzureichen.
- Die betreffende Zentralbank prüft die Anträge und leitet sie an die EZB weiter. Vorbehaltlich eines anders lautenden, den Teilnehmern mitzuteilenden Beschlusses des EZB-Rates werden alle eingegangenen Anträge innerhalb von 14 Wochen nach Auftreten der technischen Störung beurteilt.
- Die betreffende Zentralbank teilt den jeweiligen Teilnehmern das Ergebnis der Beurteilung mit. Wird aufgrund dieser Beurteilung ein Ausgleichsangebot gemacht, so müssen die betreffenden Teilnehmer das Angebot in Bezug auf jede/n in ihrem Antrag enthaltene/n Zahlung oder Zahlungsauftrag innerhalb von vier Wochen nach Übermittlung des Angebots durch Unterzeichnung eines Standard-Annahmeschreibens, dessen jeweils aktuelle Fassung auf der Website der betreffenden Zentralbank abrufbar ist, annehmen oder ablehnen. Geht der betreffenden Zentralbank innerhalb von vier Wochen kein Annahmeschreiben zu, so gilt dies als Ablehnung des Ausgleichsangebots durch die jeweiligen Teilnehmer.
- Die betreffende Zentralbank leistet die Ausgleichszahlungen nach Erhalt des Annahmeschreibens des TARGET2-Nutzers. Auf Ausgleichszahlungen werden keine Zinsen erstattet.

Anhang I SSP Interregionale Ausfallsicherung mit Datenverlust

Wiederherstellungsprozess

Gemäß den drei Anbieter-Zentralbanken (3ZB) ist ein Wiederherstellungsprozess in Region 2 nur dann erforderlich, wenn beide Standorte in Region 1 gleichzeitig ausfallen und es daher zu einem Datenverlust kommt. **Durch die Wiederherstellung soll gewährleistet werden, dass alle in Region 1 verarbeiteten Nachrichten auch in Region 2 angezeigt werden.** Zu diesem Zweck werden alle Nachrichten, die in Region 1 in den zwei Minuten vor der Störung verarbeitet wurden, wiederholt und mit den in Region 2 angezeigten Nachrichten abgestimmt, um möglicherweise fehlende Nachrichten zu identifizieren.

Möglicherweise fehlen könnten beispielsweise FIN-Nachrichten (Zahlungen und Liquiditätstransfers einschließlich solcher, die über die T2S-Schnittstelle (T2SI) an bzw. von Geldkonten gesendet wurden, sowie FileAct-Nachrichten (die von einem Nebensystem über eine Nebensystemschnittstelle (ASI) gesendet wurden), oder InterAct-Nachrichten (XML-Nachrichten, die auf eines der SSP-Module oder an die T2SI gesendet wurden).

Der Wiederherstellungsprozess sollte in folgenden Schritten ablaufen:

1) FIN-Nachrichten können wiederholt und der FIN-Nachrichtenverkehr abgestimmt werden (dies würde 80 % des fehlenden Nachrichtenverkehrs ausmachen).

   Nach Abruf der FIN-Nachrichten (wobei DCA-Nachrichten unberücksichtigt bleiben) werden alle zusammengehörenden FIN-Nachrichten (sich entsprechende Nachrichten MT 096 und MT 097) in Region 2 verbucht, während alle nicht zusammengehörenden Nachrichten in Region 2 in eine Warteschlange gestellt werden. Zusammengehörende FIN-Nachrichten, die in Region 1 als final eingestuft wurden, jedoch aufgrund der fehlenden Erfassung nicht in Region 2 verbucht werden konnten, werden als neu ausstehende Zahlungen („newly pending payments“) angezeigt. Der SSP Service Desk kennzeichnet alle ausstehenden Zahlungen als sehr dringend („highly urgent“) und stellt sie ganz vorne in die Warteschlange der sehr dringenden Zahlungen ein.

2) Der SSP Service Desk informiert den TARGET2 Coordination Desk über die Beendigung des vorangegangenen Schritts.

3) Zur Synchronisierung des Umsatzes und der Salden zwischen PM-Konten und Geldkonten stimmt der TARGET2 Coordination Desk die Positionen auf beiden Euro-Zwischenkonten ab und identifiziert die fehlenden Zahlungen (die im TARGET2-Zwischenkonto auf der T2S-Plattform verarbeitet wurden und im T2S-Zwischenkonto auf der SSP fehlen).[1]

   Nach Durchführung der Identifizierung informiert der TARGET2 Coordination Desk die Zentralbanken über die fehlenden Liquiditätstransfers; jene sollten ihrerseits die betroffenen Teilnehmer über die beeinträchtigten Liquiditätsübertragungen sowie über die zu ergreifenden Maßnahmen unterrichten.

Folgende Schritte sind denkbar:

- Bei **Liquiditätstransfers von PM-Konten auf Geldkonten**, die auf T2S und der SSP (Region 1) vor dem Katastrophenfall, jedoch nicht auf der SSP (Region 2) nach dem Katastrophenfall gebucht wurden, wird die für den Inhaber des belasteten Geldkontos zuständige Zentralbank das betreffende PM-Konto belasten und die Gutschrift nach Autorisierung durch den PM-Geldkontoinhaber auf das T2S-Zwischenkonto vornehmen. Hat sich der Inhaber des PM-Kontos für Anzeigen der Kontobelastungen entschieden, sollte die Nachricht im Zusammenhang mit der erneuten Buchung über den vorherigen Schritt ignoriert werden.

- Bei **Liquiditätsübertragungen von Geldkonten auf PM-Konten**, die in T2S und auf der SSP (Region 1) vor dem Katastrophenfall, jedoch nicht in der SSP (Region 2) nach dem Katastrophenfall gebucht wurden, wird die für das belastete Geldkonto zuständige Zentralbank die ausgehenden liquiditätstransferbezogenen Nachrichten ermitteln und sie erneut senden (über GUI Screen Cash > Liquidity > Immediate Liquidity Transfers > Search/List Screen > Related Outbound Messages > Resend). Falls sich der Inhaber des PM-Kontos für Gutschriftsanzeigen entschieden hat, sollte die Nachricht zu der über den vorangegangenen Schritt erneut erfolgten Buchung ignoriert werden.

Die vorgenannten Schritte sollten innerhalb von zwei Stunden nach dem Beschluss einer Ausfallsicherung abgeschlossen sein.

[1] TARGET2 und T2S sollten den Geschäftstag nicht abschließen, bevor nicht die Zwischenkonten synchronisiert wurden. Doch am Tagesende könnte T2S, falls die DCA-Salden bei null stehen, die Selbstbesicherung zurückbezahlt ist und die TARGET2-Zwischenkonten null betragen, den Geschäftstag abschließen, selbst wenn die SSP nach einen Katastrophenfall vor einen Neustart steht. Dabei sollte aber sichergestellt werden, dass zuvor alle erforderlichen Nachrichten von T2S erneut an die SSP gesendet werden (die Nachrichten sollten in die Warteschlange gestellt und dann von der SSP verarbeitet werden.

4) Nach Beendigung der vorherigen Schritte sollte eine Telefonkonferenz der TARGET2-Settlement-Manager abgehalten werden, um sich über die Initiierung des erneuten Versands der InterAct- und FileAct-Nachrichten (die rund 20 % des fehlenden Nachrichtenverkehrs ausmachen) abzustimmen. Der SSP Service Desk öffnet die Gemeinschaftsplattform für SWIFTNet-Dienste, also FileAct und InterAct.

5) Die Nebensysteme sollten sämtliche innerhalb zehn Minuten vor der Störung in Region 1 versendeten FileAct-Nachrichten, bzw. die vom Nebensystem als fehlend identifizierten Dateien, mit demselben Betreff erneut verschicken. Des Weiteren müssen die Nebensysteme, Banken und Zentralbanken ihren InterAct-Nachrichtenverkehr der letzten beiden Minuten vor dem Vorfall wiederholen (außer bei Nachrichten in Verbindung mit Liquiditätstransfers an/von Geldkonten). Neue FileAct- und InterAct Nachrichten sollten hingegen nicht versendet werden. Durch die Öffnung der Gemeinschaftsplattform für SWIFTNet erhalten die Teilnehmer auch Zugang zum Informations- und Steuerungsmodul (ICM), um den Bearbeitungsstatus zu prüfen.

6) Durch die Bearbeitung der fehlenden FileAct- und InterAct-Nachrichten dürften sich die neu ausstehenden Zahlungen („newly pending payments“) weiter verringern. Verbleibende neu ausstehende Zahlungen sollten von den Zentralbanken „forciert“ werden; hierdurch wird bestätigt, dass diese Zahlungen in Region 1 final waren und in Region 2 final bleiben sollten. Auf diese Weise würde jedes sich daraus ergebende Restrisiko beim Eurosystem liegen. Entsprechend sollten verbleibende neu ausstehende AS-Transaktionen, die in Region 1 final waren, in Region 2 final bleiben und daher „forciert“ werden. Um die Existenz „neu ausstehender AS-Transaktionen” anzuzeigen, müsste das Nebensystem Belege an die entsprechende Zentralbank liefern, wonach diese Transaktionen in Region 1 final waren (z. B. eine Kopie der erhaltenen Benachrichtigung).

7) Nachdem der SSP Service Desk dem TARGET2 Coordination Desk bestätigt hat, dass alle neu ausstehenden Zahlungen abgewickelt wurden, wird eine Telefonkonferenz zwischen den Krisenmanagern abgehalten, um deren Zustimmung zur Öffnung der Gemeinschaftsplattform für FIN-Nachrichten zu erhalten. Alle in der Warteschlange stehenden FIN-Zahlungen werden abgewickelt. Dann können die Nutzer auch neue FileAct- und Inter Act-Nachrichten senden. Wurde das CM genutzt, dann findet der Saldenübertrag für SWIFTNet FIN-Nachrichten vom CM zum PM nach Schließung des CM und nach Öffnung der Gemeinschaftsplattform statt.

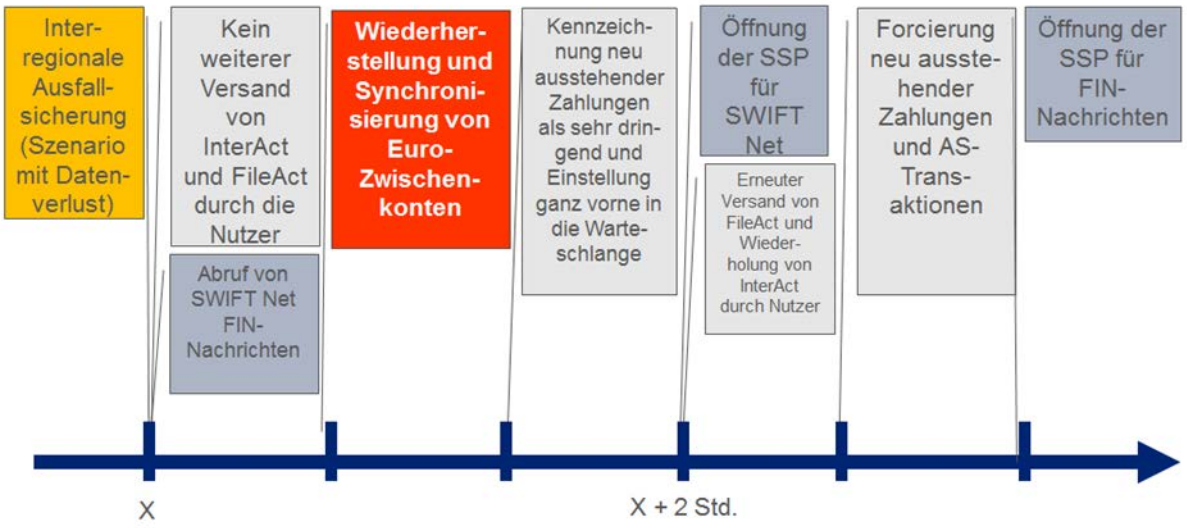

Inter-regionale Ausfall-sicherung (Szenario mit Daten-verlust)
Kein weiterer Versand von InterAct und FileAct durch die Nutzer
Abruf von SWIFT Net FIN-Nachrichten
Wiederher-stellung und Synchroni-sierung von Euro-Zwischen-konten
Kennzeich-nung neu ausstehender Zahlungen als sehr drin-gend und Einstellung ganz vorne in die Warte-schlange
Öffnung der SSP für SWIFT Net
Erneuter Versand von FileAct und Wieder-holung von InterAct durch Nutzer
Forcierung neu ausste-hender Zahlungen und AS-Trans-aktionen
Öffnung der SSP für FIN-Nachrichten
X
X + 2 Std.

Abbildung 20: Abläufe nach einer interregionalen Ausfallsicherung mit Datenverlust

Anhang II Störungsbericht für TARGET2-Nutzer

Vertraulichkeit

Die in diesem Dokument enthaltenen Informationen werden vom Eurosystem ausschließlich dazu verwendet, die Ausfallsicherheit des TARGET2-Systems insgesamt zu erhöhen. Innerhalb des Eurosystems werden diese Informationen nur an Personen weitergegeben, die sie aus dienstlichen Gründen benötigen.

Name der verantwortlichen Zentralbank	

Angaben zu den Ansprechpartnern	
Name des TARGET2-Nutzers	
Name des Ansprechpartners	
Titel/Funktion	
Telefonnummer	
E-Mail-Adresse	

Grundsätzliche Angaben zum Vorfall	
Identifikationsnummer des Vorfalls (wird von der verantwortlichen Zentralbank vergeben)	**CC/JJJJMMTT/Nr.**

Status	☐ Vorläufig ☐ Final[2]
Art der fehlerhaften Komponente	☐ Hardware ☐ Software[3] ☐ Netzwerk[4] ☐ Infrastruktur[5] ☐ Menschliches Versagen
Datum und Uhrzeit des Störungsbeginns (MEZ)	ttmmjjjj / ss.mm
Datum und Uhrzeit des Störungsendes (MEZ)	ttmmjjjj / ss.mm
Dauer	ss.mm

[2] Ein Störungsbericht gilt als „final“, wenn das Umsetzungsdatum der Abhilfemaßnahme angezeigt wird.

[3] Software bezieht sich auf Systemsoftware (einschließlich Datenbanksystemen) und Anwendersoftware.

[4] Dies betrifft lediglich das interne Netzwerk. Ausfälle des externen Netzwerks sind unter Infrastruktur aufzuführen.

[5] Die Infrastruktur umfasst Grundstücke und Gebäude sowie unterstützende Dienstleistungen (wie Klimatisierung, Stromversorgung, Telekommunikation (einschließlich SWIFT)).

Beschreibung des Vorfalls (Die Zusammenfassung sollte möglichst allgemeinsprachlich auf eine für die Unternehmensleitung angemessene Art verfasst werden. Die Zusammenfassung sollte beispielsweise folgende Elemente enthalten: • eine allgemeine Beschreibung des Vorfalls und seiner Auswirkungen, • die betroffenen Dienstleistungen bzw. Systeme und • die externen Auswirkungen (z. B. andere betroffene TARGET2-Nutzer)

Einzelheiten zur Störungsursache (insbesondere zur Kernursache des Vorfalls (wer, was, wo, wann, wie?))

Abhilfemaßnahmen (dieser Abschnitt sollte Punkte enthalten wie z. B.: • Maßnahmen zur Behebung des Vorfalls und • Maßnahmen zur Verhinderung einer Wiederholung des Vorfalls (Umsetzung geplant bis…))

_____

Datum und Unterschrift
Name des Unterzeichners (Druckschrift)
Funktion:

Dieses Formular ist an die oben genannte Zentralbank zurückzusenden:

Anschrift	
Kontaktperson	

Anhang III Selbstzertifizierungserklärung

Einleitung

Die Prinzipien für Finanzmarktinfrastrukturen weisen den Betreibern von Zahlungssystemen bestimmte Verantwortlichkeiten zu, denen sie nachkommen müssen. So bezieht sich beispielsweise Prinzip 17 auf Aspekte im Zusammenhang mit der Sicherheit und der Zuverlässigkeit des Betriebs von Finanzmarktinfrastrukturen wie beispielsweise systemrelevanten Zahlungssystemen.

Prinzip 17 besagt, dass „ein FMI für seine Teilnehmer die Einführung von betrieblichen Mindestanforderungen erwägen sollte. So könnte ein FMI je nach Rolle und Systemrelevanz eines Teilnehmers Betriebs- und Business-Continuity-Anforderungen für seine Teilnehmer definieren."

Vor diesem Hintergrund hat das Eurosystem in seiner Funktion als Betreiber des TARGET2-Systems eine Gruppe von Anforderungen zum Informationssicherheits- und Business-Continuity-Management erarbeitet, die von den kritischen Teilnehmern von TARGET2 erfüllt werden müssen. Kritische Teilnehmer können den Umsetzungsgrad dieser Anforderungen gemäß nachfolgender Anlage zertifizieren. Der EZB-Rat stimmte diesem Konzept am 25. Oktober 2007 zu (SEC/GovC/07/041).

Anforderungen zum Informationssicherheits- und Business-Continuity-Management

1. **Informationssicherheitsmanagement**

Kritische Teilnehmer müssen die Sicherheit ihrer TARGET2-Schnittstellenkomponenten und sonstiger Komponenten, die hinter der Schnittstelle liegen, aber von wesentlicher Bedeutung für einen reibungslosen Zahlungsfluss sind, beurteilen. In den Anforderungen sind auf übergeordneter Ebene die von den kritischen Teilnehmern umzusetzenden Prinzipien zum Informationssicherheitsmanagement vereint. Die Prinzipien wurden von dem international vereinbarten Standard ISO/IEC 27002 abgeleitet.

Anforderung 1.1: Informationssicherheitspolitik

Die Geschäftsführung sollte einen klaren sicherheitspolitischen Kurs festlegen, der im Einklang mit den Geschäftszielen steht; darüber hinaus sollte sie sich zur Informationssicherheit verpflichten und diese fördern, indem sie eine in der gesamten Organisation geltende Strategie ausarbeitet und aufrechterhält.

Anforderung 1.2: Interne Organisation

Um die Umsetzung einer Informationssicherheitsstrategie innerhalb der Organisation anzustoßen und zu überwachen, sollte ein Steuerungsrahmen geschaffen werden. Die Geschäftsführung sollte der

Informationssicherheitsstrategie zustimmen, Sicherheitsrollen zuweisen sowie die Implementierung der entsprechenden Strategie innerhalb der gesamten Organisation koordinieren und überprüfen.

Anforderung 1.3: Externe Parteien

Die Sicherheit der Informationen und informationsverarbeitenden Stellen einer Organisation sollte nicht durch die Einführung von Produkten externer Parteien verringert werden. Der Zugang externer Parteien zu den informationsverarbeitenden Stellen der Organisation sollte in jedem Fall kontrolliert werden. Sofern externe Parteien einen Zugang benötigen oder Produkte und Dienstleistungen externer Parteien erforderlich sind, sollte eine Risikoprüfung erfolgen, um die sicherheitsrelevanten Auswirkungen zu ermitteln und die Kontrollanforderungen zu bestimmen. Die Kontrollen sollten mit der externen Partei vereinbart und vertraglich festgelegt werden.

Anforderung 1.4: Vermögensverwaltung (Asset Management)

Alle organisationseigenen Werte sollten erfasst und einem Eigentümer namentlich zugeordnet sein. Die Zuständigkeit für die Aufrechterhaltung angemessener Kotrollen sollte festgelegt werden. Der Eigentümer kann, soweit angemessen, die Durchführung bestimmter Kontrollen delegieren, er ist jedoch weiterhin für den ordnungsgemäßen Schutz der organisationseigenen Werte verantwortlich.

Anforderung 1.5: Klassifizierung von Informationen

Damit ersichtlich ist, ob, mit welcher Priorität und in welchem Umfang Informationen während ihrer Verwendung zu schützen sind, sollte eine Klassifizierung der Informationen vorgenommen werden. Mithilfe eines Informationsklassifizierungsschemas sollten angemessene Schutzstufen definiert und die Notwendigkeit spezieller Maßnahmen im Umgang mit bestimmten Informationen kommuniziert werden.

Anforderung 1.6: Personelle Sicherheit

Die Verantwortlichkeiten bezüglich der Sicherheit sollten bereits vor der Einstellung von Mitarbeitern in einer entsprechenden Stellenbeschreibung benannt und in den jeweils geltenden vertraglichen Bedingungen festgehalten werden. Alle Nutzer, bei denen es sich um Bewerber, Vertragspartner und Dritte handelt, sollten hinreichend überprüft werden, besonders bei sensiblen Stellen bwz. Aufträgen. Bewerber, Vertragspartner und Dritte, die Informationsverarbeitungssysteme nutzen, sollten eine Vereinbarung, in der ihre Sicherheitsrollen und Verantwortlichkeiten festgelegt sind, unterzeichnen. Es sollte gewährleistet sein, dass alle Mitarbeiter, Vertragspartner und Dritte hinreichend für den Sicherheitsaspekt sensibilisiert sind. Zur Minimierung möglicher Sicherheitsrisiken sollten sie an Fortbildungen und Schulungen zu Sicherheitsverfahren und dem korrekten Einsatz der informationsverarbeitenden Einrichtungen teilnehmen. Es sollte ein formelles Disziplinarverfahren

geschaffen werden, das bei Verletzung von Sicherheitsbestimmungen zur Anwendung kommt. Das Ausscheiden eines Mitarbeiters, Vertragspartners oder Dritten bzw. dessen Wechsel innerhalb der Organisation muss durch Zuweisung entsprechender Verantwortlichkeiten im Hinblick auf etwaige Sicherheitsaspekte gesteuert werden, und es ist zu gewährleisten, dass sämtliche Betriebsmittel zurückgegeben und alle Zugangsberechtigungen entzogen werden.

Anforderung 1.7: Physische und umgebungsbezogene Sicherheit

Kritische oder sensible informationsverarbeitende Einrichtungen sind in Sicherheitsbereichen unterzubringen, die durch eine genau festgelegte Sicherheitszone sowie entsprechende Sicherheitsbarrieren und Zutrittskontrollen geschützt sind. Sie sollten physisch vor unrechtmäßigem Zutritt sowie Zerstörung und Manipulation geschützt sein.

Die Betriebsmittel sollten vor physischen und umgebungsbezogenen Bedrohungen geschützt werden. Um das Risiko eines unerlaubten Zugriffs auf Informationen zu mindern sowie Schäden und Verluste zu verhindern, ist es erforderlich, dass sämtliche Betriebsmittel (auch solche, die nicht am Standort verwendet werden) und das Entfernen von Eigentum geschützt sind. Zur Abwehr physischer Bedrohungen und zum Schutz der unterstützenden Infrastruktur wie der Stromversorgung und der Verkabelung können Sondermaßnahmen erforderlich sein.

Anforderung 1.8: Betriebs- und Kommunikationsmanagement

Für die Verwaltung und den Betrieb sämtlicher informationsverarbeitender Einrichtungen sind Verantwortlichkeiten und Verfahren festzulegen. Was die Betriebsprozesse betrifft, so sollte bei Bedarf eine Aufteilung der Verantwortlichkeiten vorgenommen werden, um das Risiko eines fahrlässigen oder vorsätzlichen Systemmissbrauchs zu verringern.

Die Organisation sollte in Bezug auf externe Dienstleistungsanbieter prüfen, ob Vereinbarungen bestehen, überwachen, ob diese eingehalten werden, und Änderungen weiterverfolgen, damit gewährleistet ist, dass die erbrachten Leistungen alle mit dem Dritten vereinbarten Anforderungen erfüllen.

Um die Verfügbarkeit der für die benötigte Systemleistung ausreichenden Kapazität und Ressourcen sicherzustellen, müssen im Vorfeld Pläne ausgearbeitet und Vorbereitungen getroffen werden. Zur Reduzierung des Risikos einer Systemüberlastung sollten Vorabberechnungen zu den künftigen Kapazitätsanforderungen angestellt werden. Die betrieblichen Anforderungen an neue Systeme sind festzulegen, zu dokumentieren und vor ihrer Abnahme und Verwendung zu testen.

Es müssen Maßnahmen getroffen werden, um den Eintritt von Schadsoftware und nicht autorisiertem mobilen Programmcode zu verhindern bzw. aufzudecken. Für Software und informationsverarbeitende Einrichtungen besteht die Gefahr, dass sie durch das Eindringen von Schadsoftware wie Computerviren, Netzwerkwürmern, trojanische Pferden und logischen Bomben geschädigt werden. Die Nutzer sollten für diese Gefahren sensibilisiert werden. Die verantwortlichen Personen sollten Mechanismen einrichten, wo dies angemessen erscheint, um das Eindringen von Schadsoftware zu verhindern bzw. aufzudecken und diese Software zu entfernen, sowie Maßnahmen zur Kontrolle von mobilem Programmcode treffen.

Es müssen Routineverfahren eingerichtet werden, um die vereinbarten Backup-Maßnahmen sowie die Strategie zur Sicherung der Daten und zur Erprobung ihrer zeitnahen Wiederherstellung umzusetzen.

Um Netzwerke, die sich über eine gesamte Organisation erstrecken können, sicher zu verwalten, muss dem Datenverkehr, rechtlichen Aspekten sowie der Überwachung und dem Schutz besondere Beachtung geschenkt werden. Des Weiteren sind unter Umständen zusätzliche Kontrollmechansismen zum Schutz sensibler Daten, die über öffentliche Netzwerke geleitet werden, erforderlich.

Speichermedien sollten kontrolliert und physisch geschützt werden. Damit Dokumente, Computermedien, Ein- und Ausgabedaten sowie Systemdokumentationen nicht unerlaubt eingesehen, verändert, entfernt oder zerstört werden können, müssen entsprechende betriebliche Verfahren etabliert werden.

Ein Austausch von Informationen und Software zwischen verschiedenen Organisationen sollte auf Basis einer formellen Austauschrichtlinie erfolgen und im Rahmen von Austauschvereinbarungen durchgeführt werden. Zudem sind die einschlägigen Rechtsvorschriften einzuhalten. Verfahren und Standards sollen festgelegt werden, durch die in der Übertragung befindliche Informationen sowie physische Medien mit solchen Informationen geschützt werden.

Die Systeme sind zu überwachen und Informationssicherheitsereignisse zu melden. Es empfiehlt sich der Einsatz von Betreiberprotokollen und Fehlerprotokollen, um sicherzustellen, dass Probleme im Bereich des Informationssystems erkannt werden. Eine Systemüberwachung sollte gegeben sein, um die Effizienz der eingeführten Kontrollmechanismen zu überprüfen und die Übereinstimmung mit einem entsprechenden Zugangsmodell zu verifizieren.

Anforderung 1.9: Zugangskontrolle

Der Zugang zu Informationen, informationsverarbeitenden Einrichtungen und Geschäftsprozessen sollte auf Basis von Betriebs- und Sicherheitsanforderungen kontrolliert werden. Die Bestimmungen

zur Zugangskontrolle sollten den Regelungen zur Informationsweitergabe und Autorisierung Rechnung tragen. Um die Zuweisung von Rechten zum Zugriff auf Informationssysteme und -dienste zu kontrollieren, müssen formelle Verfahren etabliert werden. Diese Verfahren sollten den gesamten Lebenszyklus des Nutzerzugangs abdecken - angefangen von der Erstregistrierung neuer Nutzer bis hin zur endgültigen Abmeldung von Nutzern, die keinen Zugang mehr benötigen. Zu beachten ist insbesondere auch die Notwendigkeit, im Bedarfsfall die Zuweisung von Rechten zum bevorrechtigten Zugang zu kontrollieren, mit denen solche Nutzer Systemkontrollen umgehen können.

Die Nutzer sollten auf ihre Verantwortung zur Aufrechterhaltung effizienter Zugangskontrollen hingewiesen werden, insbesondere was die Verwendung von Passwörtern und die Sicherheit der Benutzerausstattung betrifft. Der Grundsatz des aufgeräumten Schreibtischs und leeren Bildschirms sollte umgesetzt werden, um das Risiko eines unberechtigten Zugangs oder der Beschädigung von Unterlagen, Medien und informationsverarbeitenden Einrichtungen zu verringern.

Der Zugang zu internen wie auch externen vernetzten Diensten ist zu kontrollieren. Wenn Nutzer Zugang zu Netzwerken und Netzwerkdiensten erhalten, darf dies nicht die Sicherheit der Netzwerkdienste beeinträchtigen, d. h, es sollte gewährleistet werden, dass geeignete Schnittstellen zwischen dem Netzwerk der Organisation und den Netzwerken anderer Organisationen und öffentlichen Netzwerken eingerichtet sind, geeignete Authentisierungsverfahren für Nutzer und Betriebsmittel angewandt wer- den und die Zugangskontrollen zu den Informationsdiensten umgesetzt werden.

Die Sicherheitseinrichtungen sollten so eingesetzt werden, dass der Zugang zu Betriebssystemen nur autorisierten Nutzern gewährt wird. Diese Einrichtungen sollten in der Lage sein, autorisierte Nutzer zu authentisieren, erfolgreiche und fehlgeschlagene Systemauthentisierungsversuche aufzuzeichnen, die Verwendung spezieller Systemsonderrechte zu dokumentieren und Alarm auszulösen, wenn Systemsicherheitsbestimmungen verletzt werden; des Weiteren sollten geeignete Authentisierungsmöglichkeiten vorhanden sein, und die Verbindungszeit der Nutzer sollte gegebenenfalls begrenzt werden können. Der logische Zugriff auf die Software und die Informationen einer Anwendung sollte auf autorisierte Nutzer beschränkt werden.

Beim Einsatz des Mobile Computing sollte das Risiko, das mit der Arbeit in einer ungeschützten Umgebung einhergeht, besonders berücksichtigt und für geeigneten Schutz gesorgt werden. Bietet die Organisation Telearbeit an, sollten Schutzmaßnahmen am Telearbeitsplatz getroffen werden, und es sollte gewährleistet sein, dass geeignete Vorkehrungen für diese Arbeitsmethode bestehen.

Anforderung 1.10: Beschaffung, Entwicklung und Wartung von Informationssystemen

Zu Informationssystemen zählen Betriebssysteme, Infrastruktur, Branchenanwendungen, Standardanwendungen, Dienste und von Nutzern entwickelte Programme. Vor der Entwicklung und/oder Implementierung von Informationssystemen sollten die Sicherheitsanforderungen ermittelt und vereinbart werden.

Zur Gewährleistung einer korrekten Verarbeitung sollten geeignete Kontrollen in die Anwendungen, auch in solche, die von Benutzern entwickelt wurden, integriert werden. Die Validierung von Ein- und Ausgabedaten und intern verarbeiteten Daten sollte Bestandteil dieser Kontrollen sein. Zusätzliche Kontrollen sind eventuell für Systeme erforderlich, die sensible, wertvolle oder kritische Informationen verarbeiten oder diese beeinflussen. Solche Kontrollen sind auf Basis der Sicherheitsanforderungen und einer Risikoprüfung festzulegen.

Es sollte eine Leitlinie zur Anwendung von Kryptografie entwickelt werden, um die Vertraulichkeit, Authentizität und Integrität von Informationen zu schützen. Zur Unterstützung derartiger Maßnahmen sollte die Verwaltung kryptografischer Schlüssel geregelt sein.

Der Zugang zu Systemdateien und Quellcode sollte kontrolliert werden; IT-Projekte und Supportmaßnahmen sind in sicherer Form durchzuführen. Die Organisation sollte dafür sorgen, dass sensible Daten in Testumgebungen nicht frei zugänglich sind. Projekt- und Supportumgebungen sind einer strengen Kontrolle zu unterstellen.

Für den Umgang mit Schwachstellen sollten effiziente, systematische und reproduzierbare Verfahren entwickelt werden, deren Wirksamkeit durch Messungen bestätigt wird. In diese Überlegungen sollten alle Betriebssysteme und verwendeten Anwendungen einbezogen werden.

Anforderung 1.11: Umgang mit Informationssicherheitsvorfällen

Es sollte ein formelles Melde- und Eskalationsverfahren für entsprechende Ereignisse geben. Alle Mitarbeiter, Vertragspartner und externen Nutzer sollten auf die Meldeverfahren für die verschiedenen Arten von Ereignissen und Schwachstellen, die Einfluss auf die Sicherheit der organisationseigenen Werte haben könnten, hingewiesen werden. Sie sollten verpflichtet werden, sämtliche Informationssicherheitsereignisse und Schwachstellen so schnell wie möglich den dafür benannten Anlaufstellen zu melden. Um Informationssicherheitsereignisse und Schwachstellen effizient und unmittelbar nach ihrer Meldung beheben zu können, sollten entsprechende Verantwortlichkeiten und Verfahren festgelegt werden. Das Reagieren auf Informationssicherheitsereignisse sowie deren Überwachung, Auswertung und allgemeine Handhabung sollte in einem fortlaufenden Prozess kontinuierlich verbessert werden.

Anforderung 1.12: Erfüllung

Die Ausgestaltung, der Betrieb, der Einsatz und die Verwaltung von Informationssystemen können gesetzlichen, aufsichtsrechtlichen und vertraglichen Sicherheitsanforderungen unterliegen. Die Organisation sollte bezüglich der besonderen rechtlichen Anforderungen die Unterstützung ihres Rechtsberaters oder eines geeignet qualifizierten Juristen in Anspruch nehmen.

Die Sicherheit der Informationssysteme ist regelmäßig zu überprüfen. Diese Überprüfungen sollten im Einklang mit den jeweiligen Sicherheitsbestimmungen erfolgen. Die technischen Plattformen und Informationssysteme sollten einer Revision unterzogen werden, um festzustellen, ob die geltenden sicherheitsrelevanten Implementierungsstandards und die dokumentierten Sicherheitskontrollen eingehalten werden. Während der Revision von Informationssystemen sind die Betriebssysteme und die Revisionswerkzeuge durch Kontrollen zu schützen. Schutzmaßnahmen sind auch erforderlich, um die Integrität der Revisionswerkzeuge zu schützen und ihren Missbrauch zu verhindern.

2**. Business-Continuity-Management**

Jeder Nutzer, der vom Eurosystem im Hinblick auf das reibungslose Funktionieren von TARGET2 als kritisch eingestuft wurde, muss über eine Strategie zur Aufrechterhaltung des Geschäftsbetriebs verfügen, die folgende Elemente aufweist:

Anforderung 2.1: Business-Continuity-Pläne wurden erstellt, und Verfahren zu deren Einhaltung sind vorhanden.

Anforderung 2.2: Es muss ein Ausweichstandort vorhanden sein.

Anforderung 2.3: Das Risikoprofil des Ausweichstandorts muss sich von dem des Primärstandorts unterscheiden. Dies bedeutet, dass sich der Ausweichstandort a) in deutlicher Entfernung vom Primärstandort befinden muss und b) nicht von denselben Komponenten[6] der physischen Infrastruktur abhängen darf.[7] Dadurch wird das Risiko, dass beide Standorte von derselben Störung betroffen sind,

6 Zu beachten ist, dass keine Verpflichtung zur Nutzung unterschiedlicher Hardware-Marken und/oder Software-Komponenten besteht, z. B. zur Installation von MS Windows am (eigentlichen) Primärstandort und von UNIX-Systemen am Ausweichstandort. Die Aussage „nicht von denselben Komponenten der physischen Infrastruktur abhängen“ unterstreicht, dass Ausweichstandorte nicht auf die Infrastrukturkomponenten (z. B. Transport, Telekommunikation, Wasser- und Energieversorgung) angewiesen sein sollten, die am Primärstandort genutzt werden.

7 Hierbei wird berücksichtigt, dass TARGET2-Nutzer lediglich für Dinge, die in ihren direkten Einflussbereich fallen, verantwortlich sein können. Sie sind zum Teil von den Anbietern abhängig und nicht haftbar, wenn sich die Ausfallsicherheit eines von Dritten bereitgestellten Dienstes als weniger verlässlich erweist als erwartet. TARGET2-Nutzer sollten jedoch bestrebt sein, die Festlegung einer angemessenen Ausfallsicherheit in dem mit den Anbietern geschlossenen Vertrag sicherzustellen. So sollte sich z. B. ein Telekommunikationsanbieter im Rahmen der vertraglichen Vereinbarungen verpflichten, mehrere Routing-Einrichtungen bereitzustellen.

minimiert. So sollte beispielsweise der Ausweichstandort an ein anderes Energieversorgungsnetz und eine andere Hauptfernmeldeleitung als der Primärstandort angeschlossen sein.[8]

Anforderung 2.4: Im Falle einer größeren Betriebsstörung, die dazu führt, dass auf den Primärstandort nicht zugegriffen werden kann und/oder für den Betrieb notwendige Mitarbeiter nicht verfügbar sind, muss der kritische Teilnehmer in der Lage sein, den normalen Betrieb vom Ausweichstandort aus wiederaufzunehmen und dort den Geschäftstag ordnungsgemäß abzuschließen und den/die folgenden Geschäftstag(e) zu beginnen.

Anforderung 2.5: Es müssen Verfahren etabliert sein, die gewährleisten, dass die kritischsten Transaktionen während der Verlagerung vom Primärstandort auf den Ausweichstandort ausgeführt werden können.

Anforderung 2.6: Die Fähigkeit, Betriebsstörungen zu bewältigen, wird mindestens einmal jährlich geprüft, und wichtige Mitarbeiter werden in geeigneter Weise geschult. Der Abstand zwischen den Tests sollte nicht länger als ein Jahr sein.

Feststellung des Umsetzungsgrades

Für jede der oben aufgeführten Anforderungen dokumentiert der kritische Teilnehmer in der Anlage zu dieser Selbstzertifizierung, inwieweit diese bereits umgesetzt wurden.

Im Falle der Nichtumsetzung einer der obigen Anforderungen (Stufe 2 oder 3) sollten in der Anlage die größten Risiken[9] beschrieben werden. Darüber hinaus ist ein Aktionsplan zur Behebung des Problems beizufügen, wobei auch das vorgesehene Umsetzungsdatum für jede einzelne Maßnahme aufzuführen ist. Diese Angaben sind auszuwerten, und die Durchführung der Maßnahmen zur Risikominderung ist von der zuständigen Zentralbank zu überwachen.

Kontaktdaten

In der nachstehenden Tabelle sind Name und Kontaktdaten der Person aufzuführen, die einzuschalten ist, wenn weitere Informationen benötigt werden.

[8] Basierend auf den „High-level principles for business continuity“, erarbeitet von: The Joint Forum, Bank für Internationalen Zahlungsausgleich, August 2006.

[9] Ein großes Risiko könnten beispielsweise unzureichende Vorkehrungen gegen Denial-of-Service-Angriffe, eine nicht vorhandene unterbrechungsfreie Stromversorgung u. ä. sein.

Name des kritischen Teilnehmers	
Anschrift	
Kontaktperson (Name) (Druckschrift)	
Kontaktperson (Tel.-Nr.)	
Kontaktperson (E-Mail)	

Unterzeichner

Die Selbstzertifizierung ist von einer Führungskraft (auf Vorstandsebene oder einer vergleichbaren Ebene) zu unterzeichnen, die beim kritischen Teilnehmer für den entsprechenden Geschäftsbereich verantwortlich ist. Angesichts der wichtigen Rolle, die der Informationstechnologie (IT) zukommt, sollte die Selbstzertifizierung zusätzlich von einer Führungskraft (ebenfalls auf Vorstands- oder vergleichbarer Ebene) aus dem IT-Bereich des kritischen Teilnehmers unterzeichnet werden. Wenn eine Führungskraft sowohl für den Geschäfts- als auch den IT- Bereich zuständig ist, reicht eine Unterschrift aus.

Zertifizierung

Die Unterzeichner bestätigen, dass sie die in dieser Selbstzertifizierungs-Erklärung aufgeführten Anforderungen gelesen und verstanden haben. Die Erklärung (nebst Anlage) gilt für ein Jahr und muss spätestens ein Jahr nach dem Datum der ersten Unterschrift verlängert werden.

Die Unterzeichner zertifizieren, dass die in der Anlage enthaltenen Informationen ein zutreffendes und genaues Bild der aktuellen Situation vermitteln. Sie bestätigen ferner, dass die Anlage unter ihrer Leitung und Kontrolle erstellt wurde und die ausgewiesenen Angaben von qualifiziertem Personal ordnungsgemäß erhoben und ausgewertet wurden. Alle Angaben sind nach bestem Wissen und Gewissen der Unterzeichner korrekt, akkurat und vollständig. Den Unterzeichnern ist bekannt, dass die Einreichung dieser Daten eine wesentliche Verpflichtung bedeutet und die Einreichung falscher, ungenauer oder irreführender Angaben einen Verstoß gegen Artikel 34 Absatz 2 Buchstabe c darstellt, was einer der Gründe für eine Beendigung der Teilnahme des betreffenden Instituts an TARGET2 ist.

Die Unterzeichner bestätigen ferner, dass es in ihrer Organisation einen Mechanismus gibt, der sicherstellt, dass die Einhaltung der Anforderungen im folgenden Jahr gewährleistet bleibt, oder - sofern die Maßnahmen noch nicht vollständig umgesetzt wurden - dass angemessene Vorkehrungen getroffen werden, die zufriedenstellende Fortschritte bei der Durchführung der im Aktionsplan aufgeführten Punkte ermöglichen.

Erste Unterschrift

Name der Führungskraft aus dem Geschäftsbereich (Druckschrift)	
Titel:	
Datum:	
Unterschrift:	

Zweite Unterschrift

Name der Führungskraft aus der IT-Abteilung (Druckschrift)	
Titel:	
Datum:	
Unterschrift:	

Dieses Formular (einschließlich Anlage) bitte zurücksenden an (von der zuständigen Zentralbank auszufüllen):

Name der Zentralbank:	
Anschrift:	
Kontaktperson:	

Anlage zur Selbstzertifizierungserklärung

Name des kritischen Teilnehmers …….

1. **Umsetzungsgrad**

Die kritischen Teilnehmer sind verpflichtet anzugeben, inwieweit die vom Eurosystem in seiner Funktion als TARGET2-Systembetreiber festgelegten Anforderungen zum Informationssicherheitsmanagement und zum Business-Continuity-Management umgesetzt wurden.

Durch Ankreuzen der entsprechenden Kästchen geben die Unternehmen bekannt, inwieweit die Vorgaben umgesetzt wurden.

- Vollständige Umsetzung: Der kritische Teilnehmer hat alle Anforderungen wie in der Selbstzertifizierungs-Erklärung aufgeführt umgesetzt.
- Stufen der Nichtumsetzung:
    - **Stufe 1:** keine wesentlichen Bereiche der Nichtumsetzung; es kann mit hinreichender Sicherheit davon ausgegangen werden, dass dies nicht zu einer Beeinträchtigung der reibungslosen Funktion von TARGET2 und/oder negativen Auswirkungen auf andere Systemteilnehmer führen wird.
    - **Stufe 2:** wesentliche Bereiche der Nichtumsetzung; eine Zusicherung wie in Stufe 1 kann nicht gegeben werden; eine Ausnutzung der ermittelten Schwachstellen könnte zu einer Beeinträchtigung der reibungslosen Funktion von TARGET2 und/oder negativen Auswirkungen auf andere Systemteilnehmer führen.
    - **Stufe 3:** Nichtumsetzung; eine Zusicherung wie in Stufe 1 kann nicht gegeben werden; eine Ausnutzung der ermittelten Schwachstellen würde zu einer erheblichen Beeinträchtigung der reibungslosen Funktion von TARGET2 und/oder negativen Auswirkungen auf andere Systemteilnehmer führen.

Anforderungen	Vollständige Umsetzung	Nichtumsetzung		
		Ebene 1	Ebene 2	Ebene 3
1. Informationssicherheitsmanagement				
Anforderung 1.1	☐	☐	☐	☐
Anforderung 1.2	☐	☐	☐	☐
Anforderung 1.3	☐	☐	☐	☐
Anforderung 1.4	☐	☐	☐	☐
Anforderung 1.5	☐	☐	☐	☐
Anforderung 1.6	☐	☐	☐	☐
Anforderung 1.7	☐	☐	☐	☐
Anforderung 1.8	☐	☐	☐	☐
Anforderung 1.9	☐	☐	☐	☐
Anforderung 1.10	☐	☐	☐	☐
Anforderung 1.11	☐	☐	☐	☐
Anforderung 1.12	☐	☐	☐	☐
Welcher Informationssicherheitsstandard wird für Sicherheitskontrollen hauptsächlich verwendet?				
2. Business-Continuity-Management				
Anforderung 2.1	☐	☐	☐	☐
Anforderung 2.2	☐	☐	☐	☐
Anforderung 2.3	☐	☐	☐	☐
Anforderung 2.4	☐	☐	☐	☐
Anforderung 2.5	☐	☐	☐	☐
Anforderung 2.6	☐	☐	☐	☐

2. **Umsetzungsfortschritt**

Sofern Bereiche der Nichtumsetzung gemäß Stufe 2 oder 3 ermittelt wurden, ist auch der folgende Abschnitt auszufüllen.

Wurden Risiken infolge einer Nichtumsetzung der Anforderungen 1.1 bis 1.12 und 2.1 bis 2.6 (gemäß Stufe 2 oder 3) ermittelt? Kommentare:
Welche Schritte werden eingeleitet, damit eine vollständige Umsetzung der Anforderungen erreicht wird bzw. der Grad der Nichterfüllung nur noch der Stufe 1 entspricht? Kommentare:
Bis zu welchem Datum soll die vollständige Umsetzung erreicht werden bzw. der Grad der Nichterfüllung nur noch der Stufe 1 entsprechen? Kommentare

Anhang IV Formular für Änderungsvorschläge

Memo für Vorschläge zur Änderung der SSP
Absender:_____ NZB des Absenders:_____
Datum:_____

Angaben zur Änderung	
Bezeichnung der Änderung	Kurze Erläuterung
Priorität nach Einschätzung des Nutzers	Mögliche Optionen: hoch, mittel, niedrig
Betroffene Module	Sofern bekannt. Mögliche Optionen: PM, ICM, SD, HAM, SFM, RMM, ASI, T2S-Schnittstelle (mehrere Angaben möglich)
Beschreibung der Änderung	
Derzeitiges Systemverhalten	Bezieht sich der Vorschlag auf eine bestehende oder eine neue Dienstleistung? Angabe der betroffenen bestehenden Dienstleistung (Hinweise zu den UDFS und/oder zum ICM-Benutzerhandbuch erbeten)
Vorgeschlagene Änderung - Funktionsbeschreibung	Funktionsbeschreibung der neuen/verbesserten Dienstleistung Angabe, ob Nutzung der vorgeschlagenen Änderung optional oder obligatorisch ist (sofern zutreffend)
Geschäftsvorfall und erwartetes Ergebnis nach Umsetzung der Änderung	Beschreibung des dem Vorschlag zugrunde liegenden Geschäftsvorfalls sowie des Nutzens durch die Umsetzung
Begleitdokumente	
1 Dokument	Weitere Anlagen wie Bildschirmausdrucke, Flussdiagramme usw.
2 Dokument	Erläuternde Beispiele

Anmerkung: Im Feld „Vorgeschlagene Änderungen“ sollte die Funktionsbeschreibung so genau wie möglich sein, mit klaren Regeln, die keinen Raum für Interpretationen lassen.

Anhänge

Anhang V Glossar und Abkürzungsverzeichnis

A B C D E F G H I J K L M N P R S T U V W X Y Z

-A- Glossar

Akkreditierte Zertifizierungsstelle (accredited certification authority)**:**

Eine oder mehrere Zentralbanken, die vom EZB-Rat dazu bestimmt wurden, im Rahmen des internetbasierten Zugangs bei der Ausstellung, Verwaltung, dem Widerruf und der Erneuerung elektronischer Zertifikate für das Eurosystem tätig zu werden.

Algorithmus (algorithm)**:**

Ein Algorithmus ist eine mathematische Methode, um eine reibungslose, schnelle und liquiditätssparende Verarbeitung der Zahlungen in einer Warteschlange zu gewährleisten, beispielsweise, indem gegeneinander aufrechenbare Zahlungsströme berücksichtigt werden.

Application-to-Application (A2A):

Verbindungsmodus, der den Informationsaustausch zwischen den Softwareanwendungen der SSP und der T2S-Plattform und den Softwareanwendung(en) der Nutzer ermöglicht.

AS Contingency Tool:

Das „AS Contingency Tool“ ist ein Instrument für das Nebensystem zur Vereinfachung der Generierung und Verarbeitung von XML-Nachrichten. Es steht ausschließlich Zentralbanken zur Verfügung.

Ausfallsicherung (failover**):**

Eine Ausfallsicherung bezeichnet die Möglichkeit, technisch von einem Standort auf einen zweiten umzuschalten. Innerhalb der Konfiguration der Gemeinschaftsplattform gibt es zwei Ausfallsicherungssituationen:

- Intraregionale Ausfallsicherung: Überwechseln von einem Standort zu einem zweiten Standort innerhalb derselben Region
- Interregionale Ausfallsicherung: Überwechseln von einer Region zu einer anderen

-B- **Glossar**

Batch

Ein Batch ist ein Stapel von Aufträgen (Zahlungs- und/oder Wertpapierübertragungsaufträgen), der als Einheit verarbeitet wird.

Berechtigung (privilege):

Ein gewährtes oder verweigertes Recht, innerhalb einer Anwendung bestimmte Funktionen auszuführen oder auf bestimmte Daten zuzugreifen und/oder diese zu aktualisieren.

BIC

Business Identifier Code

BIC1:

Ein Nicht-SWIFT-BIC, der an der achten Stelle eine „1“ trägt. Ein BIC1 kann nicht in der Kopfzeile einer SWIFT-Nachricht verwendet werden.

BIC8:

Die ersten acht Stellen eines des BIC. Bei Adressierungen bezeichnen sie den Zielort.

BIC11:

Neben den ersten acht Zeichen des BIC wird ein dreistelliger optionaler Code zur Bezeichnung von Zweigstellen oder sonstigen Referenzangaben eines Instituts verwendet.

BIC-Directory:

Von SWIFT veröffentlichtes Verzeichnis der Identifikationscodes von Kreditinstituten.

Bruttoausgleich in Echtzeit (real-time gross settlement - RTGS):

Unter einem Bruttoausgleich in Echtzeit versteht man die kontinuierliche Übertragung von Geldern oder Wertpapieren in Echtzeit. Dabei wird jede Transaktion einzeln und ohne Netting ausgeführt.

Bruttoausgleichssystem (gross settlement system):

Übertragungssystem, bei dem jede Übertragung von Vermögenswerten oder Wertpapieren einzeln abgewickelt wird.

Business Continuity (Aufrechterhaltung des Geschäftsbetriebs):

Vorkehrungen im Zahlungsverkehrssystem zur Gewährleistung des vereinbarten Leistungsspektrums auch bei Ausfall einer oder mehrerer Systemkomponenten oder bei Auftreten eines außergewöhnlichen externen Ereignisses. Die Vorkehrungen zur Business Continuity umfassen sowohl Präventiv- als auch Notfallmaßnahmen.

-C- **Glossar**

CBT (computer-based terminal - CBT):

Computergestütztes Terminal von SWIFT

Clearing:

Als Clearing bezeichnet man das Verfahren zur Berechnung der gegenseitigen Verbindlichkeiten von Marktteilnehmern für den Austausch von Wertpapieren und Geld. Es kann auch die Übermittlung, die

Abstimmung und in einigen Fällen die Bestätigung von Zahlungs- oder Wertpapieraufträgen umfassen.

Clearinghaus (clearing house):

Eine Verrechnungsstelle, die ein Clearing-System betreibt, welches aus einem Satz von Regeln und Verfahren besteht, über das Finanzinstitute Daten und/oder Dokumente in Verbindung mit Zahlungen oder Wertpapierübertragungen an einem einzigen Ort vorlegen und untereinander austauschen. Zu den Verfahren gehört häufig auch ein Mechanismus zur Berechnung der gegenseitigen Positionen der Teilnehmer, möglicherweise auf Nettobasis, um den Ausgleich ihrer Verbindlichkeiten im Abwicklungssystem zu erleichtern.

Client Collateralisation:

Kredit, den ein DCA-Inhaber seinen Kunden in T2S im Rahmen eines Besicherungsmechanismus zur Verfügung stellt.

Closed Group of Users (CGU):

Eine Untergruppe von Kunden, die zur Verwendung der jeweiligen Dienste und Produkte des jeweiligen Mehrwertnetzdienstleisters beim Zugang zur T2S-Plattform zusammengefasst werden.

Closed User Group (CUG):

Eine Untergruppe von Kunden, die zur Verwendung der jeweiligen SWIFT-Dienste und -Produkte beim Zugang zum Zahlungsmodul zusammengefasst werden.

Contingency-Modul (contingency module - CM):

Das Contingency-Modul ist ein gemeinsames obligatorisches Instrument der Zentralbanken zur Bewältigung von Notfallsituationen, um kritische und sehr kritische Zahlungen abwickeln zu können.

Contingency-Netzwerk (contingency network):

Ein vom Eurosystem betriebenes alternatives Netzwerk zur Weiterleitung des Zahlungsverkehrs bei einem Ausfall der SWIFT-Dienste.

Contingency-Situation (contingency):

Eine Contingency-Situation bezeichnet einen eingeschränkten Geschäftsbetrieb bei einem Systemausfall. Systemisch wichtige Zahlungen werden in Contingency-Situationen auf Basis vereinbarter Contingency-Verfahren und Contingency-Kommunikationsverfahren abgewickelt.

Continuous Linked Settlement (CLS):

CLS ist ein globales Abwicklungssystem für Devisentransaktionen. Es bietet den Teilnehmern die gleichzeitige Verarbeitung beider Seiten der Transaktion und schaltet somit das Erfüllungsrisiko aus.

CRISP (consumption report and invoicing support process):

CRISP ist ein optionales Kundenbetreuungssystem der Gemeinschaftsplattform, das den nationalen Zentralbanken für die Rechnungserstellung zur Verfügung steht.

CRM (customer relationship management):

Dieser Begriff bezieht sich auf die Verwaltung kundenorientierter Angaben im Zusammenhang mit den Nutzern (Teilnehmern, Nebensystemen und anderen Kunden, beispielsweise Zentralbankkunden im Heimatkontomodul) durch die Zentralbanken.

CRSS (customer related services system):

CRSS ist eine der beiden technischen Konfigurationen der Gemeinschaftsplattform. Die andere ist das Zahlungsabwicklungs- und Kontoführungssystem PAPSS. Bei dieser technischen Konfiguration sind die ausschließlich den nationalen Zentralbanken vorbehaltenen Grundleistungen und optionalen Leistungen vollständig oder teilweise implementiert.

CRSS-Hauptmeldefunktionen (CRSS core reporting functions):

Mit Wirkung vom November 2012 wurden die „Core Requirements on Statistics and Storage“ (CROSS) und das „Customer Relationship and Knowledge of Systems“ (CRAKS1) als „CRSS Core Reporting Functions“ (CRSS-Hauptmeldefunktionen) zusammengefasst. Sie beinhalten die Dienstleistungen der Gemeinschaftsplattform für Zentralbanken, die diese u. a. für die Archivierung und Speicherung von Aktivitäten, für Rechnungskalkulationen, für die Bereitstellung von Statistiken zu Innertageskrediten und für Profilangaben verbindlich nutzen. Der Support für die Customer

Relationships and Knowledge of Payments Systems wird durch CRAKS3, ebenfalls im CRSS verfügbar, erbracht.

CSD-Teilnehmer (CSD participant):

Kunde eines Zentralverwahrers (Central Securities Depository – CSD).

-D- **Glossar**

Daueauftrag (standing order):

Auftrag, regelmäßig einen bestimmten Betrag von einem Konto auf ein anderes Konto zu überweisen.

Dediziertes Konto (dedicated account):

Konto im Zahlungsmodul, auf dem dedizierte Liquidität für die Abwicklung im Nebensystem gehalten wird. Dies kann entweder ein Unterkonto (Schnittstellen-Modell) oder ein Spiegelkonto (integriertes Modell) sein.

Dedizierte Liquidität (dedicated liquidity):

Liquidität, die auf einem Unterkonto oder einem Spiegelkonto gehalten wird, um die Abwicklung von Transaktionen im Nebensystem zu ermöglichen.

Dediziertes Zwischenkonto (dedicated transit account):

Ein im RTGS-System und in T2S geführtes Geldkonto, das vom verantwortlichen Systembetreiber unterhalten wird und der Übertragung von Geldern dient. Das in T2S geführte Zwischenkonto wird als dediziertes RTGS-Zwischenkonto (RTGS dedicated transit account) und das im RTGS-System geführte Zwischenkonto als dediziertes T2S-Zwischenkonto (T2S dedicated transit account) bezeichnet.

Direkt angeschlossener Geldkontoinhaber (directly connected DCA holder):

Ein Geldkontoinhaber, dem von der jeweiligen Zentralbank ein direkter Zugang zu T2S gewährt wurde, um die T2S-Dienstleistungen zu nutzen. Die Zentralbank fungiert nicht als technische

Schnittstelle (andernfalls wäre der Geldkontoinhaber ein „indirekt angeschlossener Geldkontoinhaber“).

Direkter Teilnehmer (direct participant):

Teilnehmer eines Systems, der direkt mit anderen Teilnehmern dieses Systems Transaktionen durchführt. Er kann alle in dem System erlaubten Tätigkeiten ohne Intermediär vornehmen. In einigen Systemen können direkte Teilnehmer auch Transaktionen im Auftrag indirekter Teilnehmer durchführen.

Dokumente, die den T2S-Umfang definieren (T2S scope-defining set of documents):

Der Umfang von T2S ist in folgenden Dokumenten definiert: User Requirement Definitions (URD), User Detailed Functional Specifications (UDFS), GUI Business Functionality, GFS Functional Chapter, Dedicated Link Connectivity Specifications und Data Migration Tool Specifications and Related Procedures.

-E- **Glossar**

Earmarking:

Kennzeichnung einer bestimmten Menge von Wertpapieren auf einem Wertpapierkonto, die nur für bestimmte Arten von Transaktionen oder Prozessen zugelassen ist. Ein CSD-Teilnehmer kann beispielsweise eine Wertpapierposition auf einem Wertpapierkonto oder alle auf dem Konto verbuchten Wertpapiere alsbesicherungsfähige Sicherheiten kennzeichnen.

EBA Clearing (EBA):

Unternehmen, das im Auftrag seiner Mitglieder das EURO1-und das STEP2-Verrechnungssystem unterhält.

Ebene 1 (level 1):

EZB-Rat

Ebene 2 (level 2):

Zentralbanken des Eurosystems

Ebene 3 (level 3):

Anbieter-Zentralbanken

Echtzeit-Bruttosystem (RTGS-System) (real-time gross settlement system):

Ein Echtzeit-Bruttosystem ist ein Abwicklungssystem, bei dem Verarbeitung und Ausgleich in Echtzeit und auf Bruttobasis erfolgen. Ein RTGS-System kann ein zentrales Warteschlangenverfahren für Aufträge bereitstellen, die nicht zum Zeitpunkt der Einreichung bearbeitet werden können (beispielsweise weil nicht genügend Liquidität vorhanden oder das Liquiditätslimit ausgeschöpft ist).

(Effekten-)Girosystem (book-entry system):

System, das die Übertragung von Wertpapieren und anderen Finanzinstrumenten gestattet, ohne effektive Stücke zu bewegen (z. B. die elektronische Übertragung von Wertpapieren).

Einlagefazilität (deposit facility):

Ständige Fazilität des Eurosystems, die den Geschäftspartnern die Möglichkeit bietet, Guthaben bis zum nächsten Geschäftstag zu einem vorher festgesetzten Zinssatz bei einer nationalen Zentralbank anzulegen.

Endgültige Abwicklung (final settlement):

Die endgültige Abwicklung ist die Erfüllung einer Verpflichtung durch eine Übertragung von Geldern und von Wertpapieren, die unwiderruflich, unumkehrbar und unaufhebbar geworden ist.

Ersatzzahlungen (backup payments):

Wenn das System eines PM-Kontoinhabers nicht mehr verfügbar ist, kann dieser mithilfe von Ersatzzahlungen seinen Zahlungsverpflichtungen gegenüber CLS und EURO1 nachkommen und eine Liquiditätskonzentration auf seinem PM-Konto verhindern. Solche Ersatzzahlungen werden über das Informations- und Steuerungsmodul (ICM) initiiert. Dabei stehen zwei Arten von Ersatzzahlungen zur Verfügung:

- Contingency-Zahlungen zur Erfüllung von Einzahlungsverpflichtungen gegenüber CLS, dem EURO1-Sicherheitenkonto oder dem EURO1-Deckungskonto (TARGET2/EURO1-Liquiditätsbrücke)
- Ersatzzahlungen zur Umverteilung von Liquidität, durch die überschüssige Liquidität, die sich auf dem PM-Konto des betreffenden Teilnehmers angesammelt hat, verteilt wird.

ESZB (ESCB):

Europäisches System der Zentralbanken

EU:

Europäische Union

Eurosystem:

Die EZB und die nationalen Zentralbanken der EU-Mitgliedstaaten, deren Währung der Euro ist, wie in Artikel 1 der Satzung des ESZB und der EZB festgelegt.

EWR (EEA):

Europäischer Wirtschaftsraum

External Guarantee Limit:

Vom Geldkontoinhaber für seinen Kunden festgelegte Obergrenze für Kredite, die außerhalb von T2S besichert werden. Das External Guarantee Limit und das Unsecured Credit Limit sind aus der Sicht von T2S identisch. Sie unterscheiden sich nur hinsichtlich der Reihenfolge ihrer Inanspruchnahme, wobei die Client Collateralisation genutzt wird, nachdem das External Guarantee Limit ausgeschöpft wurde.

EZB (ECB):

Europäische Zentralbank

-F- **Glossar**

Fernzugangsteilnehmer (remote participant):

Direkter Teilnehmer der Gemeinschaftsplattform, der in dem Land, über das er an der Gemeinschaftsplattform teilnimmt, keine Vertretung hat.

FIFO-Prinzip (first in, first out):

Zahlungsaufträge werden in der Reihenfolge ihres Eingangs ausgeführt (d. h. der zuerst eingegangene Zahlungsauftrag wird als erstes bearbeitet, der zuletzt eingegangene Auftrag zum Schluss). Maßgeblich ist der Zeitstempel des Zahlungsauftrags beim Eingang in der SWIFT-Schnittstelle der Gemeinschaftsplattform.

FIFO-Überhol-Prinzip (FIFO by-passing):

Das System versucht, den ersten Auftrag in der Warteschlange zu bearbeiten. Ist dies aufgrund fehlender Deckung nicht möglich, versucht das System, stattdessen den nächsten Auftrag abzuwickeln. Dieser Vorgang wird FIFO-Überhol-Prinzip genannt.

-G- **Glossar**

Garantiekonto (guarantee funds account):

Konto auf der Gemeinschaftsplattform, das zur Bereitstellung oder zur Anforderung von Liquidität für den Saldenausgleich eines Nebensystems bei Ausfall der Verrechnungsbank(en) gehalten wird.

Garantiekonto-Verfahren (guarantee fund mechanism):

Verfahren, um nach vorab festgelegten Regeln zusätzlich benötigte Liquidität bereitzustellen, wenn die Abwicklung über ein Nebensystem allein anhand der Liquidität der Verrechnungsbank nicht möglich ist.

Geldkonto (dedicated cash account - DCA):

Ein in den Büchern einer Zentralbank geführtes T2S-Geldkonto.

Geldkonto-Inhaber (DCA holder):

Eine Stelle, die bei einer Zentralbank mindestens ein Geldkonto in T2S eröffnet hat.

Gemeinschaftsplattform (single shared platform - SSP):

TARGET2 basiert auf einer einzigen technischen Plattform, der Gemeinschaftsplattform, die sowohl das Zahlungsabwicklungs- und Kontoführungssystem PAPSS als auch das Kundenbetreuungssystem CRSS umfasst.

Gespeicherter Zahlungsauftrag (warehoused payment):

Zahlungsauftrag, der bis zu fünf TARGET2-Geschäftstage im Voraus eingereicht wird. Die Zahlungsnachricht wird dann bis zur Tagverarbeitung der Gemeinschaftsplattform an dem betreffenden Tag gespeichert.

Grafische Benutzeroberfläche (Graphical User Interface – GUI):

Schnittstelle, die dem Nutzer eine Interaktion mit der T2S-Softwareanwendung ermöglicht, indem grafische Elemente (z. B. Fenster, Menüs, Schaltflächen und/oder Icons) auf einem Computerbildschirm per Tastatur und Maus angesteuert werden.

GUI-Nachricht (broadcast via GUI):

Die Übermittlung einer Information, die einer bestimmten Gruppe von Teilnehmern zeitgleich auf der grafischen Benutzeroberfläche zur Verfügung gestellt wird.

-H- **Glossar**

Hauptbuch (general ledger):

Das Hauptbuch ist das zentrale Rechnungslegungsdokument eines Unternehmens, das auf dem Prinzip der doppelten Buchführung beruht.

Heimatkonto (home account):

Von nationalen Zentralbanken gehaltenes Konto außerhalb des Zahlungsmoduls, z. B.

- für Einrichtungen, die nicht den Status eines direkten PM-Teilnehmers haben können
- für Einrichtungen, die PM-Konten eröffnen dürfen und indirekte PM-Teilnehmer sind (oder die weder als direkte noch als indirekte Teilnehmer am Zahlungsmodul teilnehmen)
- für PM-Kontoinhaber zum Zwecke der Abwicklung von Vorgängen, die nicht im Zahlungsmodul verarbeitet werden

Die Heimatkonten werden über das Heimatkontomodul oder über ein proprietäres Heimatkontosystem verwaltet.

Heimatkontomodul (home accounting module - HAM):

Das Heimatkontomodul ist ein optionales Modul. Beschließt eine Zentralbank, dieses Modul zu verwenden, stehen ihr und ihren Kunden verschiedene standardisierte Kontodienste zur Verfügung.

-I- Glossar

ICM-Nachricht (broadcast via ICM):

Die Übermittlung einer Information, die allen Teilnehmern oder einer bestimmten Gruppe von Teilnehmern zeitgleich im ICM zur Verfügung gestellt wird.

Informations- und Steuerungsmodul (information and control module - ICM):

Das Informations- und Steuerungsmodul ist eine obligatorische und einheitliche funktionale Schnittstelle zwischen den direkten Teilnehmern und dem Zahlungsmodul (PM) sowie den anderen optionalen Modulen wie dem (PM):

- Heimatkontomodul (HAM),
- Modul für die Mindestreserveverwaltung (RM),
- Modul für die ständigen Fazilitäten (SF),
- Stammdatenmodul (SD).

Innertageskredit (intraday credit):

Kreditgewährung mit einer Laufzeit von weniger als einem Geschäftstag. In einem Überweisungssystem mit Zahlungsausgleich zum Tagesabschluss werden Innertageskredite stillschweigend durch das empfangende Kreditinstitut verlängert, wenn dieses einen Zahlungsauftrag akzeptiert und auf dieser Grundlage agiert, auch wenn es die Mittel erst am Ende des Geschäftstages endgültig erhält. Innertageskredit gibt es als besicherten Überziehungskredit, Kreditgeschäft gegen Pfand oder mit Rückkaufsvereinbarung.

Innertagesliquidität (intraday liquidity):

Liquidität, die während des Geschäftstages zugänglich ist und genutzt wird, um Finanzinstituten Zahlungen auf Innertagesbasis zu ermöglichen.

Integrität (integrity):

Schutz vor zufälliger oder betrügerischer Verfälschung im Weiterleitungs- oder Speicherprozess bzw. das Wissen, ob Verfälschungen vorgenommen wurden oder nicht.

Internetbasierter Zugang (internet-based access):

Vereinbarung, im Rahmen derer ein Teilnehmer ein PM- oder HAM-Konto mit ausschließlichem Zugang über das Internet unterhält; in diesem Fall werden Zahlungs- und Kontrollnachrichten an die Gemeinschaftsplattform über das Internet übermittelt.

ISO 20022:

Internationaler Nachrichtenstandard für Finanzdienstleistungen, der von der International Organization for Standardization (ISO) festgelegt wurde.

-J- **Glossar**

Juristische Person (legal entity):

Kreditinstitut, das über einen oder mehrere Teilnehmer/Konten im Zahlungsmodul und/oder Heimatkontomodul direkt an der Gemeinschaftsplattform teilnimmt (auch Nebensysteme, wenn diese

als direkte Teilnehmer teilnehmen). Dies ermöglicht eine Gruppierung allgemeiner Informationen zu diesem Kreditinstitut im Stammdatenmodul.

-K- **Glossar**

Kontengruppe (group of accounts):

Siehe „Liquiditätspooling“.

Korrespondenzzentralbank-Modell (correspondent central banking model - CCBM):

Vom Europäischen System der Zentralbanken (ESZB) eingerichtetes Verfahren mit dem Ziel, den Geschäftspartnern die grenzüberschreitende Nutzung von Sicherheiten, die in einem anderen Land hinterlegt sind, für eine Kreditaufnahme bei der nationalen Zentralbank in dem Land, in dem sie selbst niedergelassen sind, zu ermöglichen. Beim Korrespondenzzentralbank-Modell fungieren die nationalen Zentralbanken in Bezug auf Wertpapiere in ihren nationalen Wertpapierabwicklungssystemen füreinander als Verwahrer.

Kreditinstitut (credit institution - CI):

Eine „Bank“ im Sinne der Definition der Europäischen Union. Laut erster Bankenrichtlinie der EG ist ein Kreditinstitut ein Unternehmen, dessen Tätigkeit darin besteht, Einlagen oder andere rückzahlbare Gelder des Publikums entgegenzunehmen und Kredite für eigene Rechnung zu gewähren.

Kreditlinie (credit line)

Die maximale besicherte Überziehung eines PM-Kontos. Die jeweiligen PM-Kontoinhaber können sich anhand des Informations- und Steuerungsmoduls über Veränderungen ihrer Kreditlinien informieren. Veränderungen der Kreditlinien werden unverzüglich umgesetzt. Bei einer Herabsetzung der Kreditlinie bleibt diese Änderung vorerst schwebend, wenn die Senkung zu einer ungedeckten Überziehung führen würde. Die Änderung wird wirksam, sobald die Überziehung durch die gesenkte Kreditlinie gedeckt wird.

Krisenmanager(crisis manager):

In jeder Zentralbank gibt es einen Krisenmanager, der für die Bewältigung außergewöhnlicher Ereignisse zuständig ist.

Kritische Zahlung (critical payment):

Siehe Kasten 4.

-L- **Glossar**

Ländercode (country code - CC):

Ein aus zwei Buchstaben bestehendes Kürzel zur Identifizierung des Landes, in dem die betreffende Einrichtung ansässig ist. Ländercodes werden beispielsweise im SWIFT BIC (fünfte und sechste Stelle) des BIC8 und BIC11 verwendet.

Lastschrift (direct debit):

Autorisierte Belastung des Bankkontos des Zahlungspflichtigen, die vom Zahlungsempfänger ausgelöst wird.

Lieferung gegen Zahlung (L/Z) (delivery versus payment – DVP):

Verbindung zwischen dem Wertpapierübertragungs- und dem Überweisungssystem, die sicherstellt, dass die Lieferung dann und nur dann erfolgt, wenn die Zahlung zustande kommt.

Lieferung mit Gegenwertverrechnung (delivery with payment – DwP):

Ein Weisungs- und Abwicklungsverfahren, das die Lieferung von Wertpapieren und die Leistung der entsprechenden Zahlung erfordert.

Lieferung ohne Gegenwertverrechnung (delivery free of payment – DFP oder DFOP):

Lieferung von Wertpapieren, bei der keine Übertragung entsprechender Mittel erfolgt.

Limit (limit):

Betrag, den ein direkter PM-Teilnehmer bereit ist, für normale Zahlungen an einen anderen direkten Teilnehmer (bilaterales Limit) oder die anderen direkten Teilnehmer (multilaterales Limit, sofern kein bilaterales Limit gesetzt wurde) zu zahlen, ohne vorher Zahlungen (also Gutschriften) erhalten zu haben. Direkte Teilnehmer können ständige oder aktuell laufende bilaterale (bzw. multilaterale) Limite festsetzen.

Normale Zahlungen können nur abgewickelt werden, wenn das jeweilige Limit nicht überschritten wird. Das Setzen von Limiten ist nur gegenüber PM-Kontoinhabern auf der Gemeinschaftsplattform möglich (bei einer Kontengruppe: nur gegenüber dem virtuellen Konto). Gegenüber teilnehmenden Zentralbanken kann kein Limit gesetzt werden. Eingehende dringende Zahlungen eines direkten Teilnehmers, gegenüber dem ein bilaterales/mutilaterales Limit gesetzt wurde, beeinflussen auch die bilaterale/multilaterale Position.

Liquiditätspooling (liquidity pooling functionality):

Dienstleistung basierend auf dem Konzept, dass es direkten Teilnehmern ermöglicht werden soll, ihre PM-Konten zu einer Kontengruppe zusammenzulegen. Eine solche Kontengruppe besteht aus einem Konto oder mehreren Konten eines oder mehrerer direkter PM-Teilnehmer mit einer Kapital- und/oder Management-Verbindung. Die folgenden beiden Optionen werden angeboten: virtuelle Konten (nur für Teilnehmer aus dem Euro-Währungsgebiet) und konsolidierte Information (steht auch Teilnehmern aus Ländern außerhalb des Euro-Währungsgebiets zur Verfügung).

Liquiditätsübertragung (liquidity transfer):

Überweisung von Geldern zwischen Konten desselben direkten Teilnehmers oder zwischen zwei Konten einer Kontengruppe.

Die Liquiditätsübertragung stellt auch ein Standard-Abwicklungsverfahren (Verfahren 1) dar, bei dem Liquidität von einem Spiegelkonto auf das PM-Konto einer Verrechnungsbank oder umgekehrt transferiert wird.

Es gibt zwei Arten der Liquiditätsübertragung auf der Gemeinschaftsplattform:

- Laufender Auftrag: Der Transfer wird sofort nach Auftragseingang ausgeführt, sofern ausreichend Liquidität verfügbar ist.

- Dauerauftrag: Feste Beträge werden regelmäßig zu einem bestimmten Zeitpunkt transferiert, z. B. Liquiditätszuführungen von HAM-Konten auf PM-Konten zu Beginn des Geschäftstages. Die Änderung eines Dauerauftrags wird am folgenden Geschäftstag wirksam.

Es gibt drei Arten der Liquiditätsübertragung auf der T2S-Plattform:

- Auftrag zur sofortigen Liquiditätsübertragung (immediate liquidity transfer order): Weisung, einen bestimmten Geldbetrag in Echtzeit, d. h. unmittelbar bei Eingang der Weisung, von einem Geldkonto auf ein anderes Geldkonto zu übertragen.
- Vorab erstellter Auftrag zur Liquiditätsübertragung (predefined liquidity transfer order): Weisung, einen bestimmten Geldbetrag von einem Geldkonto auf ein anderes Geldkonto zu übertragen, wobei die Weisung einmalig zu einem festgelegten Zeitpunkt oder bei Eintreten eines bestimmten Ereignisses auszuführen ist.
- T2S-Dauerauftrag zur Liquiditätsübertragung (T2S standing liquidity transfer order): Weisung, einen bestimmten Geldbetrag von einem Geldkonto auf ein anderes Geldkonto zu übertragen, wobei die Weisung so lange regelmäßig zu einem festgelegten Zeitpunkt oder bei Eintreten eines bestimmten Ereignisses im T2S-Verarbeitungszyklus auszuführen, bis der Auftrag geändert wird.

-M- **Glossar**

MAC:

Message Authentication Code

Mandated Payment:

Zahlung, die von einer nicht an der Transaktion beteiligten Stelle (typischerweise einer nationalen Zentralbank oder einem Nebensystem in Verbindung mit einem AS-Abwicklungsverfahren) im Auftrag einer anderen Stelle veranlasst wird. Beispielsweise versendet eine nationale Zentralbank eine mit einer spezifischen Nachrichtenstruktur versehene Überweisung im Auftrag eines ausgefallenen direkten Teilnehmers (nur in Contingency-Situationen). „Mandated payments“ auf technische Konten sind nicht möglich

Mindestreservepflicht (reserve requirement):

Verpflichtung der Kreditinstitute im Euro-Währungsgebiet, auf einem Mindestreservekonto Mindestreserven bei ihrer nationalen Zentralbank zu unterhalten. Die Mindestreservepflicht wird in Bezug auf bestimmte Positionen in der Bilanz der Kreditinstitute bestimmt. Die Mindestreserveguthaben der Institute werden zum Satz für die Hauptrefinanzierungsgeschäfte des Eurosystems verzinst.

Mindestreservezins- und -strafzinskonto (RM interest and penalty account):

Von einer nationalen Zentralbank gehaltenes (optionales) Konto für Buchungen im Zusammenhang mit der Zahlung von Zinsen auf Mindestreserven sowie mit der Zahlung von Strafzinsen eines Kreditinstituts, das die Mindestreserveanforderungen nicht erfüllt hat.

Modul für die Mindestreserveverwaltung (reserve management module - RM):

Das Modul für die Mindestreserveverwaltung ermöglicht es den nationalen Zentralbanken, einige Funktionen im Zusammenhang mit der Verwaltung der Mindestreserven zu nutzen. So können die Zentralbanken beispielsweise die Erfüllung des Mindestreserve-Solls überprüfen oder die an Kreditinstitute zu zahlenden Zinsen auf die Mindestreserveguthaben berechnen.

Modul für die ständigen Fazilitäten (standing facilities module - SF):

Das Modul für die ständigen Fazilitäten ist ein optionales Modul, das die Verwaltung der ständigen Übernachtfazilitäten (Einlagefazilität, Spitzenrefinanzierungsfazilität) ermöglicht.

-N- **Glossar**

Nachrichtentyp (message type - MT):

Als Nachrichtentyp bezeichnet man eine spezielle Art von SWIFT-Nachrichten, die durch eine dreistellige Zahlenfolge gekennzeichnet ist. Die erste Ziffer gibt die Nachrichtenkategorie an, aus der sich der allgemeine Zweck der Nachricht erkennen lässt. Die zweite Ziffer zeigt die Nachrichtengruppe und die dritte Ziffer die jeweilige Nachrichtenfunktion an.

Nachtverarbeitung (night-time processing):

Zeitraum, in dem AS-Transaktionen abgewickelt werden (Abwicklungsverfahren 6). Die Nachtverarbeitung dauert von 19.30 Uhr bis 7.00 Uhr (mit Ausnahme des Wartungszeitraums von 22.00 Uhr bis 1.00 Uhr).

National Service Desk:

Kontaktstelle für Banken und Nebensysteme bei ihrer nationalen Zentralbank. Der National Service Desk kümmert sich um die Belange der TARGET2-Nutzer im Hinblick auf die Nutzung der von der Gemeinschaftsplattform angebotenen Dienste und der lokalen Infrastrukturen.

Nebensystem (ancillary system - AS):

Eine der Aufsicht und/oder Überwachung durch eine zuständige Behörde unterliegende Organisation mit Sitz oder Zweigstelle im EWR, die Verrechnungs-, Zahlungs- oder Abwicklungsdienste anbietet und die Überwachungsanforderungen an den Standort der Infrastrukturen, die Dienstleistungen in Euro anbieten, in der jeweils geltenden und auf der Website der EZB veröffentlichten Fassung erfüllt; dabei werden Zahlungen und/oder Finanzinstrumente eingereicht und die daraus resultierenden Zahlungsverpflichtungen gemäß der TARGET2-Leitlinie und einer bilateralen Vereinbarung zwischen dieser Organisation und der betreffenden Zentralbank des Eurosystems über TARGET2 abgewickelt.

Nebensysteme können sein:

- Massenzahlungsverkehrssysteme
- Großbetragszahlungssysteme
- Devisensysteme
- Geldmarktsysteme
- Clearinghäuser
- Wertpapierabwicklungssysteme

Nebensystem-Schnittstelle (ancillary system interface - ASI):

Die Nebensystem-Schnittstelle ist eine standardisierte Schnittstelle zum Zahlungsmodul, über die Nebensysteme einen Zahlungsausgleich ihrer Geschäfte herbeiführen können.

Netting:

Vereinbarte Aufrechnung gegenseitiger Positionen oder Verpflichtungen von direkten Teilnehmern eines Clearing- oder Abwicklungssystems. Das Netting verringert eine große Zahl von Einzelpositionen oder -verpflichtungen auf eine kleinere Zahl. Das Netting kann verschiedene Formen annehmen, deren rechtliche Durchsetzbarkeit bei Ausfall einer der Parteien unterschiedlich ist.

Notenbankfähige Sicherheiten (eligible assets):

Vermögenswerte, die als Sicherheiten für die Kreditaufnahme verwendet werden können.

NSP (network service provider):

Netzwerkdienstleister

NUG (national user groups):

Nationale Nutzergruppen

NZB (NCB):

Nationale Zentralbank

-P- **Glossar**

PAPSS (payment and accounting processing services systems):

Zahlungsabwicklungs- und Kontoführungssystem.

Eine der beiden technischen Konfigurationen der Gemeinschaftsplattform. Die andere ist das Kundenbetreuungssystem CRSS. Folgende Module der Gemeinschaftsplattform sind im PAPSS implementiert:

- Contingency-Modul (CM)
- Heimatkontomodul (HAM)
- Informations- und Steuerungsmodul (ICM)
- Zahlungsmodul (PM), einschließlich der Schnittstelle für Nebensysteme

- Modul für die Mindestreserveverwaltung (RM)
- Modul für die ständigen Fazilitäten (SF)
- Stammdatenmodul (SD).

Teile der folgenden Dienste sind ebenfalls im Zahlungsabwicklungs- und Kontoführungssystem enthalten:

- CRISP
- CRAKS3.

Pfand (pledge):

Bereitstellung von Vermögenswerten, um die Erfüllung der Verpflichtung einer Partei (Schuldner) gegenüber einer anderen Partei (Sicherungsnehmer) zu gewährleisten. Ein Pfand räumt ein Sicherungsrecht an den übermittelten Vermögenswerten ein, wobei das Eigentum an diesen Aktiva beim Schuldner verbleibt.

PM-Konto (PM account):

Im Zahlungsmodul verwaltetes und von einem direkten Teilnehmer unterhaltenes Konto zur Abwicklung aller im Zahlungsmodul eingereichten und verarbeiteten Transaktionen (mit Ausnahme der Transaktionen im Rahmen des AS-Abwicklungsverfahrens 6, die über Unterkonten abgewickelt werden).

Priorität (priority):

Im Allgemeinen werden Zahlungen sofort abgewickelt, sofern auf dem PM-Konto des Teilnehmers ausreichend Liquidität vorhanden ist. Je nach Dringlichkeit kann der Sender diesen Zahlungen verschiedene Prioritäten zuordnen:

- sehr dringender Zahlungsauftrag (Prioritätsstufe 0)
- dringender Zahlungsauftrag (Prioritätsstufe 1)
- normaler Zahlungsauftrag (Prioritätsstufe 2).

Zahlungen, die nicht sofort abgewickelt werden können, werden ihrer Dringlichkeit entsprechend in eine Warteschlange gestellt (je eine Warteschlange für sehr dringende, dringende und normale Zahlungsaufträge). Die Prioritätsstufe kann über das Informations- und Steuerungsmodul geändert werden.

Profilinformationen (profiling information):

Den nationalen Zentralbanken zur Verfügung stehende Informationen über das Verhalten eines direkten Teilnehmers oder einer Gruppe direkter Teilnehmer in einem bestimmten Zeitraum in der Vergangenheit. Die Angaben werden zum Abgleich mit den aktuellen Daten an einem beliebigen Geschäftstag herangezogen.

Proprietäres Heimatkonto (proprietary home account - PHA):

Ein proprietäres Heimatkonto ist ein von einigen nationalen Zentralbanken unterhaltenes Konto außerhalb der Gemeinschaftsplattform, z. B. für Einrichtungen, die nicht den Status eines direkten PM-Teilnehmers haben können, für Einrichtungen, die PM-Konten eröffnen dürfen und indirekte PM-Teilnehmer sind (oder die weder als direkte noch als indirekte Teilnehmer am Zahlungsmodul teilnehmen), oder für Inhaber eines PM-Kontos zum Zwecke der Abwicklung von Vorgängen, die nicht im Zahlungsmodul abgewickelt werden. Proprietäre Heimatkonten sind nicht auf der Gemeinschaftsplattform, sondern bei den nationalen Zentralbanken angesiedelt.

-R- **Glossar**

Raw Data File:

Raw Data File

- dient als Kontrolldatei zur Überprüfung der Positionen im Hauptbuch
- kann für eigene Berichte der nationalen Zentralbanken verwendet werden.

Relationship Management Application (RMA):

Siehe SWIFT Relationship Management Application (RMA).

Reserveguthaben (reserve holdings):

Innertages- und Übernachtliquidität, die bei Tagesschluss auf einem RTGS-Konto gehalten wird.

Reservierung (reservation):

Mit der Inanspruchnahme der Liquiditätsreservierung kann der Inhaber eines RTGS-Kontos Liquidität für spezielle Transaktionen mit einer bestimmten Prioritätsstufe reservieren. HAM-Kontoinhaber können diesen Service nutzen, um Liquidität für Barabhebungen zu reservieren. Reservierungen können über das Informations- und Steuerungsmodul vorgenommen und geändert werden.

Rolle (role):

Eine Gruppe von Berechtigungen (siehe auch *Berechtigung*).

RTGS (real-time gross settlement system):

Echtzeit-Bruttosystem

Rückkaufsvereinbarung (Repogeschäft) (repurchase agreement - Repo):

Vereinbarung über den Verkauf eines Vermögenswerts und dessen Rückkauf zu einem bestimmten Preis zu einem vorher festgelegten Zeitpunkt.

-S- **Glossar**

Sehr kritische Zahlung (very critical payment)

Siehe Kasten 4.

Selbstbesicherung (auto-collateralisation):

Die Selbstbesicherung ist ein spezieller Mechanismus, um zusätzliche Liquidität für das Wertpapierabwicklungsverfahren bereitzustellen. Dieser Mechanismus beruht auf der automatischen Interaktion zwischen dem Sicherheitenverwalter, dem Wertpapierabwicklungssystem und der Gemeinschaftsplattform, um Besicherungsfunktionen (z. B. Prüfung der Notenbankfähigkeit, Bewertung von Sicherheiten) und die damit verbundene Erhöhung der Liquidität durchzuführen.

Die Selbstbesicherung wird während des Wertpapierabwicklungsverfahrens aktiviert, um der Liquiditätsknappheit eines Teilnehmers zu begegnen: Die zu übertragende Sicherheit wird im Auftrag

des Teilnehmers auf der Grundlage einer vorab erteilten Ermächtigung automatisch vom Wertpapierabwicklungssystem ausgewählt.

Die Wertpapierabwicklungssysteme verwenden derzeit zwei verschiedene Selbstbesicherungsverfahren:

- Selbstbesicherung aus Beständen: Die Teilnehmer wählen die verwendbaren notenbankfähigen Wertpapiere aus.
- Selbstbesicherung aus Strömen: Die Wertpapiere ergeben sich aus dem Abwicklungsverfahren selbst.

Settlement-Manager:

Jede Zentralbank hat einen Settlement-Manager, der für die Verwaltung und Überwachung sowie für die Kommunikation mit anderen Settlement-Managern innerhalb des Eurosystems verantwortlich ist.

Sicherheiten (collateral):

Sicherheiten sind Vermögenswerte oder die Verpflichtung eines Dritten, die vom Sicherungsnehmer zur Besicherung einer Verbindlichkeit des Sicherungsgebers gegenüber dem Sicherungsnehmer akzeptiert wird. Besicherungsvereinbarungen können verschiedene rechtliche Formen haben und als Übereignung oder Pfand auftreten.

Sicherheitenpool (collateral pool):

Vermögenswerte im Besitz der Teilnehmer eines Übertragungssystems, die diesen zu Besicherungszwecken gemeinschaftlich zur Verfügung stehen, damit sie sich nach genau festgelegten Regeln Liquidität beschaffen können.

Spiegelkonto (mirror account):

Spezielle PM-Konten, die den nationalen Zentralbanken eigens zur Nutzung von Nebensystemen zur Verfügung stehen. Spiegelkonten werden durch ein anderes im Wertpapierabwicklungssystem eröffnetes Konto gespiegelt. Im Fall einer Liquiditätsübertragung vom Konto eines direkten Teilnehmers im Zahlungsmodul auf sein Konto im Nebensystem wird der entsprechende Betrag dem Spiegelkonto belastet oder gutgeschrieben.

Spitzenrefinanzierungsfazilität (marginal lending facility):

Ständige Fazilität des Eurosystems, die die Geschäftspartner nutzen können, um sich von einer nationalen Zentralbank gegen notenbankfähige Sicherheiten Übernachtkredit zu einem im Voraus festgelegten Zinssatz zu beschaffen.

Im Allgemeinen stehen folgende Möglichkeiten zur Verfügung:

- Inanspruchnahme der Spitzenrefinanzierungsfazilität auf Antrag des direkten Teilnehmers, meist zur Erfüllung der Mindestreservepflicht.
- Automatische Inanspruchnahme der Spitzenrefinanzierungsfazilität, wobei der Innertageskredit am Ende des Tages automatisch in Übernachtkredit umgewandelt wird.

Ständige Fazilität (standing facility):

Zentralbankfazilität, die die Geschäftspartner auf eigene Initiative in Anspruch nehmen können. Das Eurosystem bietet zwei ständige Übernachtfazilitäten an, und zwar die Spitzenrefinanzierungsfazilität und die Einlagefazilität.

Stammdatenmodul (static data module - SD):

Mithilfe des Stammdatenmoduls werden die Stammdaten durch Speicherung aller tatsächlich verwendeten statistischen Daten ordnungsgemäß und zuverlässig verwaltet. Es gewährleistet die Konsistenz der Daten in allen Modulen der Gemeinschaftsplattform. Das Stammdatenmodul wird unter anderem zur Erstellung des TARGET2-Directory genutzt.

SWIFT:

Society for Worldwide Interbank Financial Telecommunication

SWIFT Alliance Access (SAA):

SWIFT Alliance Access ist eine Nachrichtenschnittstelle, die es dem Anwender ermöglicht, eigene Anwendungen mit SWIFTNet FIN (MT) und MX-basierten SWIFT-Lösungen zu verbinden.

SWIFT Alliance Gateway (SAG):

SWIFT Alliance Gateway ist das einheitliche Fenster für jede Kommunikation über SWIFTNet. Alle SWIFTNet-Nachrichtenströme können über eine Schnittstelle zusammengeführt werden. Dies betrifft

Anwendungen, die über WebSphere MQ angebunden sind, aber auch solche, die für eine Verbindung mit SWIFTNet Link bestimmt sind oder auf SWIFT Alliance WebStation basieren.

SWIFT-BIC (Business Identifier Code):

Identifikationscode von an das SWIFT-Netzwerk angeschlossenen Finanzinstituten und Unternehmen (ehemals „Bankidentifikationscode“ für Finanzinstitute).

SWIFTNet Browse:

SWIFT-Service, der auf dem Internetstandardprotokoll „https“ basiert und es den Anwendern ermöglicht, auf entfernte Web-Server zuzugreifen. Auf der Gemeinschaftsplattform gewährt die Browse-Funktion über das Secure IP Network (SIPN) von SWIFT Zugang zum Informations- und Steuerungsmodul.

SWIFTNet FileAct:

SWIFTNet FileAct ermöglicht die Übermittlung von Dateien und wird in der Regel zum stapelweisen Austausch strukturierter Finanznachrichten und umfangreicher Berichte verwendet. Auf der Gemeinschaftsplattform wird beispielweise das TARGET2-Directory mithilfe des FileAct Service über das Secure IP Network (SIPN) von SWIFT transferiert.

SWIFTNet InterAct:

Ein interaktiver Nachrichtendienst von SWIFT, der den Austausch von Nachrichten zwischen zwei Parteien unterstützt.

Auf der Gemeinschaftsplattform wird der InterAct Service verwendet, um XML-Anfragen über das Secure IP Network (SIPN) von SWIFT an das Informations- und Steuerungsmodul zu übermitteln.

SWIFT Relationship Management Application (RMA):

Von SWIFT angebotener Dienst zur Verwaltung der Geschäftsbeziehungen zwischen Finanzinstituten. Die RMA steuert, welche Nachrichtentypen zwischen den Anwendern eines SWIFT-Dienstes ausgetauscht werden dürfen.

SWIFT-Zahlungsnachricht (SWIFT payment message):

Auftrag zur Überweisung eines Geldbetrags. Der Austausch von Mitteln (Abwicklung) erfolgt anschließend über ein Zahlungssystem oder über Korrespondenzbankbeziehungen. SWIFT-Zahlungsnachrichten werden für alle Zahlungen und die damit verbundenen Transaktionen auf der Gemeinschaftsplattform eingesetzt.

-T- **Glossar**

Tagverarbeitung (day trade phase):

Als Tagverarbeitung bezeichnet man in TARGET2 die Zeit von 7.00 Uhr bis 18.00 Uhr.

TARGET:

Transeuropäisches automatisiertes Echtzeit-Brutto-Express-Zahlungssystem

TARGET2:

TARGET2 ist die zweite TARGET-Generation und ersetzt die ehemals dezentrale Infrastruktur durch eine gemeinsame technische Plattform.

TARGET2-Directory:

Von den TARGET2-Nutzern verwendetes Verzeichnis zur Adressierung von Zahlungen anhand des SWIFTNet Y-Copy Mode. Auf einzelstaatlicher Ebene kann mithilfe des Directory anhand der nationalen Bankleitzahl der zugehörige BIC ermittelt werden.

TARGET2-Geschäftstag:

TARGET2-Geschäftstage sind Kalendertage, an denen das TARGET2-System in Betrieb ist.

TARGET2-Securities (T2S):

Die Gesamtheit der Hardware-, Software- und sonstigen technischen Infrastrukturkomponenten, durch die das Eurosystem Dienstleistungen für Zentralverwahrer und Zentralbanken erbringt, die es ermöglichen, grundlegende Abwicklungsdienste in Zentralbankgeld grenzüberschreitend und marktneutral auf Basis Lieferung gegen Zahlung anzubieten.

Technisches Konto (technical account):

Konto, das im Zusammenhang mit Nebensystem-Transaktionen als Zwischenkonto verwendet wird. Darauf werden Belastungen und Gutschriften verbucht, die sich aus einem Saldenausgleich oder Transaktionen auf Basis Lieferung gegen Zahlung ergeben. Der Saldo eines solchen Kontos ist immer null, da auf Belastungen (bzw. Gutschriften) stets Gutschriften (bzw. Belastungen) in insgesamt gleicher Höhe folgen.

Technisches Konto des Nebensystems (AS technical account):

In TARGET2 angebotenes Konto zur spezifischen Nutzung von Nebensystemen.

Teilnehmer mit internetbasiertem Zugang (internet-based participant - IBP):

Teilnehmer, der über einen internetbasierten Zugang zu seinem PM- oder Heimatkonto verfügt.

Transaktionsreferenznummer (transaction reference number - TRN):

Bis zu 16-stellige alphanumerische Referenznummer, die der Sender über das SWIFT-Netzwerk gesendeten Nachrichten zuordnet.

T2S-Abwicklungswährung (T2S settlement currency):

Währung, für die T2S die Abwicklung von Wertpapiertransaktionen in Zentralbankgeld auf T2S-Geldkonten anbietet.

T2S-Beteiligter (T2S actor):

Entweder ein vertragschließender/teilnehmender Zentralverwahrer, CSD-Teilnehmer (eine juristische oder gegebenenfalls natürliche Person), der für die Zwecke der Wertpapierabwicklung in T2S ein Vertragsverhältnis zum Zentralverwahrer unterhält, eine Zentralbank, deren Währung für die abwicklungsbezogenen Aktivitäten in T2S zur Verfügung steht, oder ein Kunde einer Zentralbank, der für die Zwecke der mit der Abwicklung verbundenen Geldverrechnung in T2S ein Vertragsverhältnis zur Zentralbank unterhält.

T2S-Betreiber (T2S operator):

Die rechtliche(n) und/oder organisatorische(n) Stelle(n), die die T2S-Plattform betreibt/betreiben. Im Rahmen der Aufgabenverteilung innerhalb des Eurosystems hat der EZB-Rat die 4ZB damit beauftragt, T2S im Namen des Eurosystems zu betreiben.

T2S-Partei (T2S party):

Eine juristische Person oder Organisation, die direkt oder indirekt (d. h. über einen Zentralverwahrer oder eine Zentralbank) in T2S aktiv ist.

T2SRC (TARGET2 security requirements and controls):

TARGET2-Sicherheitsanforderungen und -kontrollen

T2S Service Desk:

Zentraler Ansprechpartner für die Zentralverwahrer, die Zentralbanken, die nicht dem Euro-Währungsgebiet angehören und ihre Währung für die Abwicklungsaktivitäten in T2S bereitstellen, die Zentralbanken des Eurosystems, die direkt angeschlossenen Teilnehmer und die Netzwerkdienstleister bei allen Vorfällen, Anfragen und Anträgen, die sich auf den Betrieb, die Funktion oder technische Aspekte von T2S beziehen. Für alle geldbezogenen Fragen, mit Ausnahme von Konnektivitätsfragen, wird auf die TARGET2-Organisationsstruktur verwiesen.

T2S-System-Entität (T2S system entity):

Entweder der Betreiber von T2S, ein Zentralverwahrer oder eine nationale Zentralbank, bei denen Verarbeitungsfunktionen und Daten voneinander getrennt sein müssen.

T2S-Systemnutzer (T2S system user):

Eine natürliche Person oder ein technischer Prozess/eine technische Anwendung, die sich mit Nutzernamen und Passwort bei T2S anmelden können. Bei einem Nutzer kann es sich z. B. um eine natürliche Person handeln, die einen interaktiven Zugang zu T2S-Online-Funktionen hat, oder um eine Anwendungssoftware, die bei T2S Dienste anfordert.

Übertragung (transfer):

Operational das Versenden (bzw. Bewegen) von Geldern oder Wertpapieren oder eines Rechts an Geldern oder Wertpapieren von einer Partei an eine andere durch: physische Übertragung von Wertpapieren/Geld, Verbuchung beim Finanzintermediär, Verbuchung in einem Überweisungs- und/oder Wertpapierübertragungssystem.

Der Akt der Übertragung wirkt sich hinsichtlich des übertragenen Geldbetrags, Wertpapiers oder Finanzinstruments auf die Rechte des Übertragenden, des Empfängers und möglicherweise auch Dritter aus.

Überweisung (credit transfer):

Geldtransfer auf Basis eines Zahlungsauftrags oder mitunter einer Reihe von Zahlungsaufträgen, um dem Empfänger finanzielle Mittel zur Verfügung zu stellen. Der Zahlungsauftrag kann über mehrere Intermediäre und/oder über ein oder mehrere Überweisungssysteme abgewickelt werden.

Unsecured Credit Limit:

Von der Payment Bank/Verrechnungsbank für ihren Kunden festgelegte Obergrenze für unbesicherte Kredite in T2S. Das External Guarantee Limit und das Unsecured Credit Limit sind aus der Sicht von T2S identisch. Sie unterscheiden sich nur hinsichtlich der Reihenfolge ihrer Inanspruchnahme, wobei das Unsecured Credit Limit genutzt wird, nachdem die Client Collateralisation ausgeschöpft wurde.

Unterkonto (sub-account):

Zu einem RTGS-Konto gehörendes spezielles Konto, auf dem dedizierte Liquidität gehalten wird, um den Ausgleich eines Nebensystems zu ermöglichen.

User Handbook (UHB):

Dokument, in dem beschrieben wird, wie T2S-Nutzer eine Reihe von T2S-Software-Funktionen nutzen können, die in einem (bildschirmbasierten) User-to-Application-Modus verfügbar sind.

User-to-Application (U2A):

Ziel ist die direkte Kommunikation zwischen den Anwendern eines Teilnehmers und dem ICM. Die Informationen werden in einem Browser angezeigt, der auf einem PC-System läuft. Kontrollen werden vom Anwender manuell vorgenommen.

-V- **Glossar**

VA-NSP (value-added network service provider):

Anbieter von Mehrwertnetzdiensten

Verfügbare Liquidität (available liquidity):

Kontoguthaben zuzüglich der besicherten Überziehungskreditlinie (falls verfügbar).

Verlängerung des Annahmeschlusses (delayed closing):

Die Verlängerung der Annahmeschlusszeit ist eine Verlängerung der Tagverarbeitung in TARGET2.

Verschlüsselung (encryption):

Als Verschlüsselung bezeichnet man den Gebrauch kryptografischer Algorithmen zur Umwandlung eines lesbaren Textes (Klartext) in einen verschlüsselten Text, um ihn vor unbefugtem Zugriff zu schützen.

Verwahrstelle (depository):

Einrichtung mit der Hauptfunktion, Wertpapiere entweder effektiv oder elektronisch zu verwahren. Die Verwahrstelle kann auch über das Eigentum an diesen Wertpapieren Buch führen.

Virtuelles Konto (virtual account):

Methode zur Aggregation von Daten innerhalb einer Gruppe von Konten, die bei einer Zentralbank im Euro-Währungsgebiet gehalten werden. Zahlungen, die von Kontoinhabern im Rahmen eines virtuellen Kontos getätigt werden, werden im Hinblick auf die Gesamtliquidität des virtuellen Kontos überprüft. Diese entspricht der Summe der verfügbaren Liquidität aller Konten, aus denen sich das virtuelle Konto zusammensetzt.

-W- **Glossar**

Warteschlangenverfahren (queuing):

Verfahren, mit dessen Hilfe Überweisungsaufträge vom sendenden direkten Teilnehmer oder vom System in einer Warteposition gehalten werden, bis sie entsprechend den Systemregeln verarbeitet werden können.

Wertpapierabwicklungssystem (securities settlement system - SSS):

Das Wertpapierabwicklungssystem umfasst die Gesamtheit aller institutionellen Regelungen für die Bestätigung, das Clearing, die Abwicklung sowie die Verwahrung und Registrierung von Wertpapieren.

-X- **Glossar**

XML:

Akronym für „Extensible Markup Language“. Untereinheit der „Standard Generalized Markup Language“ (SGML, ISO 8879), die speziell für die Verwendung im Internet sowie für webbasierte Anwendungen entwickelt wurde.

-Y- **Glossar**

Y-Copy:

Standard-Übertragungsart von SWIFT-Nachrichten an die Gemeinschaftsplattform. Sie wird bei über das Zahlungsmodul verarbeiteten Zahlungen verwendet.

-Z- **Glossar**

Zahlung (payment):

Die Gemeinschaftsplattform ermöglicht direkten Teilnehmern generell zwei Arten von Zahlungen:

- Kundenzahlungen (MT 103, MT 103+)
- Bank-an-Bank-Zahlungen (MT 202, MT 202COV, MT 204).

Zahlungsblockade (gridlock):

Situation, die sich bei einem Geld- oder Wertpapierübertragungssystem ergeben kann, wenn einige Übertragungsaufträge nicht ausgeführt werden können (weil die nötigen Geld- oder Wertpapierguthaben nicht verfügbar sind) und dies dazu führt, dass eine beträchtliche Anzahl von Aufträgen anderer Teilnehmer ebenfalls nicht ausgeführt werden kann.

Zahlungsmodul (payments module - PM):

Das Zahlungsmodul ist ein obligatorisches Modul zur Abwicklung von Zahlungen in PM-Konten, die von allen direkten Teilnehmern unterhalten werden. Darüber hinaus bietet das Zahlungsmodul erweiterte Dienstleistungen zur Liquiditätssteuerung sowie zur Kommunikation mit direkten Teilnehmern und Nebensystemen.

Zahlungsnachricht/-auftrag (payment message/instruction):

Auftrag oder Nachricht zur Übertragung von Mitteln (in Form einer Geldforderung an eine Partei) an die Order des Zahlungsempfängers. In TARGET2 kann sich der Auftrag entweder auf eine Überweisung oder auf eine Lastschrift beziehen.

Zentralbank-Selbstbesicherung (Central Bank auto-collateralisation):

Von der Zentralbank bereitgestellter besicherter Innertageskredit. Die Selbstbesicherung bei einem DCA-Inhaber wird als Client Collateralisation bezeichnet.

Zentraler Kontrahent (central counterparty - CCP):

Der zentrale Kontrahent agiert bei Handelsgeschäften an einem oder mehreren Finanzmärkten als Schaltstelle zwischen den Geschäftspartnern; dabei tritt er gegenüber jedem Verkäufer als Käufer und gegenüber jedem Käufer als Verkäufer auf.

Zentralverwahrer (central securities depository - CSD):

Eine zentrale Wertpapierverwahrstelle ist eine Einrichtung, die verbriefte und unverbriefte Wertpapiere hält, um die buchmäßige Übertragung von Wertpapieren zu ermöglichen. Neben der Verwahrung und Verwaltung von Wertpapieren kann ein Zentralverwahrer auch Clearing- und Abwicklungsfunktionen sowie Schuldendienstaufgaben wahrnehmen.